Akin

2024 Guide to DOJ and HHS OIG Guidance on Effective Compliance Programs

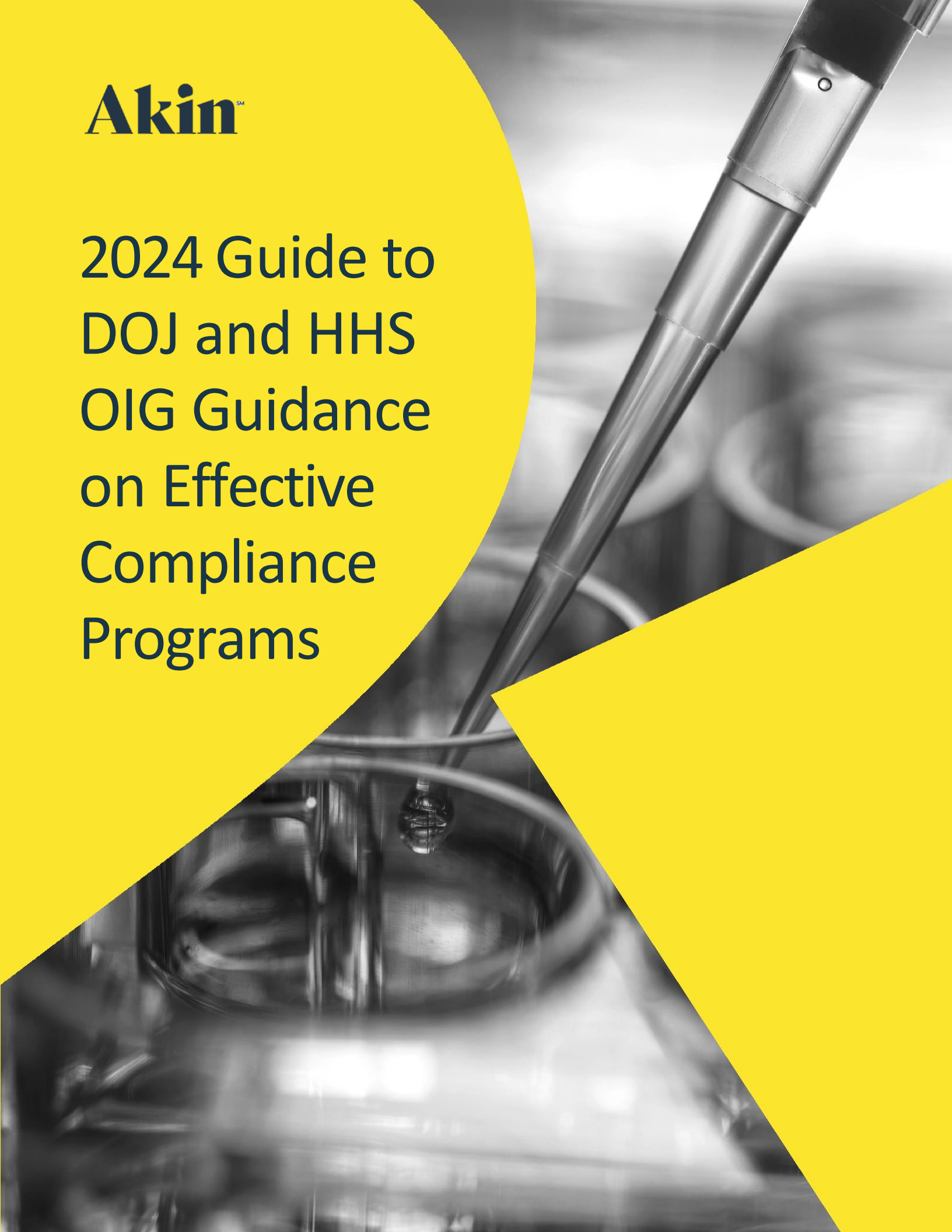


Table of Contents

Introduction

The Department of Health & Human Services' Office of Inspector General (HHS OIG) and U.S. Department of Justice (DOJ) have published important guidance and recommendations for pharmaceutical companies to develop and implement effective compliance programs. Both HHS OIG and DOJ have made it absolutely clear that robust, multifaceted compliance programs are a must for pharmaceutical companies. Akin has compiled this guide to help in-house counsel and compliance professionals navigate the evolving compliance guidance provided by both agencies.

In 2023, HHS OIG published the General Compliance Program Guidance (GCPG), providing insights which complement the 2003 Compliance Program Guidance for Manufacturers guidance. The GCPG addresses new issues such as financial arrangements, civil monetary penalties, beneficiary inducements, exclusionary authority, information blocking, Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules, and the role of compliance committees and boards of directors in ensuring compliance. It also emphasizes the inclusion of patient safety and product quality issues in compliance programs. It remains to be seen when HHS OIG might publish an update to the 2003 CPG for Manufacturers as an Industry-Specific Compliance Program Guidance.

Similarly, guidance published by the DOJ's Criminal Division helps inform prosecutors' evaluation of corporate compliance programs. The DOJ's Evaluation of Corporate Compliance Programs guidance provides a roadmap for prosecutors to assess the effectiveness of compliance programs and make informed decisions regarding resolutions, penalties, and obligations, and thus serves as a roadmap for counsel and compliance professionals in designing, maintaining and testing corporate compliance programs. The DOJ guidance has been updated multiple times, with the 2023 version introducing new considerations such as non-disclosure agreements, messaging platforms, autonomy and resources for compliance functions, compensation structures and the use of data to demonstrate program effectiveness.

We hope this guide is helpful. Companies with questions about the guidance or strategies to ensure that their compliance programs align with government expectations should contact Craig Bleifer at +1 212-872-8184 and cbleifer@akingump.com

HHS OIG's 2003 Compliance Program Guidance for Pharmaceutical Manufacturers

The Department of Health and Human Services's Office of Inspector General (HHS OIG) first issued its Draft Compliance Program Guidance (CPG) on October 3, 2002. Of note, shortly before the Draft CPG was issued, the Pharmaceutical Research and Manufacturers of America (PhRMA) had issued its own first "Code on Interactions With Healthcare Providers" effective July 1, 2002. In a nod to PhRMA's efforts, the Draft (and final) CPG specifically refer to the PhRMA Code as "a good starting point" for an effective compliance program and recommended that manufacturers "at a minimum" comply with the PhRMA Code, while noting that:

> compliance with the relevant sections of the PhRMA Code will not necessarily protect a manufacturer from prosecution or liability for illegal conduct.[1]

After a public comment period, HHS OIG published the final **OIG Compliance Program Guidance for Pharmaceutical Manufacturers [TAB 1]** on May 5, 2003, stating:

> This guidance explains the value of compliance programs and details specific elements that pharmaceutical manufacturers should consider when developing and implementing an effective compliance program.[2]

The 2003 HHS OIG Guidance was itself inspired in part by the 1987 Federal Sentencing Guidelines Manual, which set forth, with respect to mitigating factors to take into account for corporate defendants, the now well-known "7 Elements of an Effective Compliance Program", which are summarized by HHS OIG as:

1. Implementing written policies and procedures.
2. Designating a compliance officer and compliance committee.
3. Conducting effective training and education.
4. Developing effective lines of communication.
5. Conducting internal monitoring and auditing.
6. Enforcing standards through well-publicized disciplinary guidelines.
7. Responding promptly to detected problems and undertaking corrective action.[3]

---

[1] 67 Fed. Reg. 62057, at 62063.

[2] HHS OIG Announcement, "Voluntary Compliance Guidance Issued for Pharmaceutical Manufacturers," April 28, 2003, quoting Inspector General Janet Rehnquist. Available at: https://oig.hhs.gov/newsroom/news-releases-articles/voluntary-compliance-guidance-issued-pharmaceutical-manufacturers/.

[3] 68 Fed. Reg. 23731.

The 2003 Guidance was left unchanged for the next 20 years. In 2020, the HHS OIG issued the "Special Fraud Alert" on Speaker Programs,[4] which provided a great level of detail of HHS OIG's thinking on how to appropriately conduct such activities and the risks thereof, yet this was not itself an amendment to the 2003 Guidance. Then, in April 2023, HHS OIG announced that it was modernizing its CPGs, indicating that a new umbrella General CPG (GCPG) for all individuals and entities involved in the health care industry would be established, followed by industry-specific CPGs (ICPGs). OIG pointed out in its notice:

> Neither OIG's existing CPGs nor any forthcoming GCPG or ICPG constitutes a model compliance program. Rather, the goal of these documents has been, and will continue to be, to set forth a voluntary set of guidelines and identified risk areas that OIG believes individuals and entities engaged in the health care industry should consider when developing and implementing a new compliance program or evaluating an existing one.

> "Compliance program guidance is a major initiative of the OIG in its effort to engage the health care community in preventing and reducing fraud and abuse in federal health care programs. The purpose of the compliance program guidance is to encourage the use of internal controls to efficiently monitor adherence to applicable statutes, regulations and program requirements."
>
> - HHS/OIG 2003

[4] HHS OIG "Special Fraud Alert: Speaker Programs" November 16, 2020, available at https://oig.hhs.gov/documents/special-fraud-alerts/865/SpecialFraudAlertSpeakerPrograms.pdf.

HHS OIG's 2023 General Compliance Program Guidance

By November 2023, HHS OIG published the **General Compliance Program Guidance (2023 GCPG) [Tab 2]**. Keep in mind that, as a GCPG, it does not technically replace the 2003 Guidance, which is still in place.[5] There is currently no published date for the release of an ICPG for the pharmaceutical industry which will replace the 2003 Guidance. The 2023 GCPG is still instructive on many levels. Highlights of new issues tackled by the 2023 GCPG include:

- Suggestions for how to determine whether a proposed financial arrangement is violative of the Anti-Kickback Statute.
- A checklist of acts that can potentially lead to civil monetary penalties (CMPs).
- A useful summary of the Beneficiary Inducements CMP and its differences from the Federal Anti-Kickback Statute and the anti-kickback CMP, including OIG's interpretation of "remuneration" not to include items of "nominal value" of no more than $15/item or $75 in the aggregate annually.
- A detailed review of mandatory and permissive exclusionary authority of the OIG and practical ways to avoid employing or contracting with excluded persons and entities.
- Summaries of several topics not included in the 2003 Guidance at all, including managing risks relating to "Information Blocking" of electronic health information (EHI) (although most likely applicable to health information technology (IT) developers and provider entities) and HIPAA Privacy and Security Rules including breach notification requirements (although enforced by the HHS Office of Civil rights, not the OIG).
- An outline of the duties of the Compliance Committee and membership expectations, and the role of the board of directors in overseeing the compliance program.
- Suggestions for useful training topics and tactics that can create open lines of communication.
- Suggestions for potential consequences for employees who are noncompliant as well as incentives to encourage participation in the compliance program.
- A reference to the Committee of Sponsoring Organizations (COSO) Framework, the Government Accountability Office's (GAO) Green Book and the Chief Financial Officer (CFO) Council's Playbook as good examples of how to implement an adequate risk-assessment and management process as part of the compliance program.
- An emphasis on including patient safety and product quality issues in the compliance program.

[5] Thus, it would appear that the GCPG has no impact on Cal. Health & Safety Code §§ 119400-119402, which requires companies to incorporate the elements of an effective compliance program identified in the "Compliance Program Guidance for Pharmaceutical Manufacturers" published by the Office of the Inspector General, U.S. Department of Health and Human Services (HHS-OIG Guidance). Once the ICPG is published, there may be an impact.

- Suggestions for newcomers or outsiders to health care businesses, such as start-up companies, or outside investors or owners such as private equity (PE) firms.
- A review of the "7 Elements of a Successful Compliance Program" and modifications that small and larger entities might need to effectively implement a compliance program.
- The 2023 GCPG, cross-referencing recent DOJ pronouncements, also emphasizes maintenance, upkeep, electronic accessibility and comprehensibility of the company's code of conduct, policies and procedures by all "relevant individuals" including third-party contractors or agents.
- The 2023 GCPG also states that the compliance officer should not only be independent and report directly to the chief executive officer (CEO) or the board of directors but also should have the following additional characteristics that go beyond the 2003 Guidance:
    - "[H]ave sufficient stature within the entity to interact as an equal of other senior leaders of the entity" (defined as the other direct reports to the CEO).
    - "[D]emonstrate unimpeachable integrity, good judgment, assertiveness, an approachable demeanor, and the ability to elicit the respect and trust of entity employees."
    - "[H]ave sufficient funding, resources, and staff to operate a compliance program capable of identifying, preventing, mitigating, and remediating the entity's compliance risks."
    - "[S]hould not be responsible, either directly or indirectly, for the delivery of health care items and services or billing, coding, or claim submission. In addition, involvement in functions such as contracting, medical review, or administrative appeals present potential conflicts. Whenever possible, the compliance officer's sole responsibility should be compliance."
    - "[S]hould have the authority to review all documents, data, and other information that are relevant to the organization's compliance activities. This includes, but is not limited to, patient records, billing records, sales and marketing records, and records concerning the entity's arrangements with other parties, including employees, independent contractors, suppliers, physicians, and other health care professionals. The compliance officer also should have the authority to interview anyone within or connected to the organization in connection with a compliance investigation, or designate an appropriate person to conduct such an interview."

Thus, the 2023 GCPG is a good preview of things to come for the likely pharmaceutical-specific ICPG. Like the GCPG, it promises to be based on the last 20 years of experience of the OIG in prosecuting and settling cases, the conclusions reached in OIG advisory opinions on a myriad of specific proposed arrangements, and changing practices in the industry.

DOJ's 2020 "Evaluation of Corporate Compliance Programs"

The Department of Justice, Criminal Division has published several versions of the "Evaluation of Corporate Compliance Programs" (DOJ Guidance) as a way of assisting prosecutors in making decisions under the "Principles of Federal Prosecution of Business Organizations" in the Justice Manual specifically directed to issues of adequate and effective compliance programs. The DOJ Guidance document is intended to guide prosecutors as to the appropriate:

> (1) Form of any resolution or prosecution.
> (2) Monetary penalty, if any.
> (3) Compliance obligations contained in any corporate criminal resolution (e.g., monitorship or reporting obligations)[6]

The DOJ Guidance is therefore not technically directed to companies, let alone pharmaceutical companies, to require certain corporate compliance program designs, but is only a guidance for the prosecutors themselves. As stated in the DOJ Guidance:

> "This [DOJ] document is meant to assist prosecutors in making informed decisions as to whether, and to what extent, the corporation's compliance program was effective…"

However, it does provide a road map for what the DOJ and federal prosecutors will expect to see at a company, including a pharmaceutical company, in terms of demonstrating an adequate and effective compliance program. Demonstrating a program in alignment with the DOJ Guidance can allow a company to potentially avoid prosecution, obtain a more favorable resolution including potentially reduced monetary penalties and avoid new and harsh compliance program requirements, reporting and/or monitorship.

The DOJ Guidance was originally issued in February 2017 and updated in April 2019, June 2020 and finally in January 2023. These updates were based on various experiences of the DOJ in investigating, prosecuting and settling cases. The **2020 DOJ Guidance [Tab 3]** was itself a major revision of prior editions. In publishing the guidance, Assistant Attorney General Brian Benczkowski stated:

> "Effective compliance programs play a critical role in preventing misconduct, facilitating investigations, and informing fair resolutions"

[6] Evaluation of Corporate Compliance Programs (Updated March 2023), at 1.

> "Today's guidance document is part of our broader efforts in training, hiring, and enforcement to help promote corporate behaviors that benefit the American public and ensure that prosecutors evaluate the effectiveness of compliance in a rigorous and transparent manner."

The 2020 DOJ Guidance clarified and expanded upon the same three "fundamental questions" as had been posed in the previous DOJ Guidance for prosecutors when evaluating the effectiveness of a compliance program:

1. Is the Corporation's Compliance Program Well Designed?
2. Is the Program Being Applied Earnestly and in Good Faith? In other words, is the program ~~being implemented~~ adequately resourced and empowered to function effectively?
3. Does the Corporation's Compliance Program Work?

As you can see from the crossed-out language above, prior editions of the DOJ Guidance merely asked prosecutors to determine whether the program was "being implemented." By 2020, the DOJ determined (as indicated in the underlined language above) that it was critical at the highest level of analysis to determine whether the compliance program was in fact enabled to be implemented, as evidenced by the company's actual dedication of appropriate and adequate resources as well as giving the compliance function the appropriate power, authority and access necessary to perform its duties thoroughly.

Among the new areas expanded and emphasized in 2020 DOJ Guidance for a "well-designed" compliance program were:

- Training and Communications – Shorter, more targeted training sessions; and employees should be given the opportunity and means to ask questions arising out of trainings.
- Mergers and Acquisitions – Pre/post-acquisition diligence, post-acquisition remediation.
- User-Friendliness of Policies, Procedures – Tracking use/access; evaluating impact on behavior; testing awareness of/comfort with hotline.
- Autonomy and Resources – Does compliance have sufficient seniority, resources, staff, autonomy from management (be able to explain reporting structures), investment by management in training and development of compliance staff, and unfettered and adequate access to and use of company data?
- Demonstrating Effectiveness Through Data – If a company cannot demonstrate its compliance program's effectiveness through data, it will need to explain why not and whether compliance personnel were provided with the opportunity to review and analyze relevant data. The DOJ will place the onus on companies to explain any limitations on access or use of data resulting from the application of foreign laws.
- Investigation of Misconduct – Whether the company has a well-functioning and appropriately funded mechanism for timely and thorough investigations.

By 2021, however, the DOJ indicated that it was again refining its approach to corporate criminal enforcement. On October 28, 2021, Deputy Attorney General (DAG) Lisa O. Monaco restored guidance from the prior administration to require companies to provide the DOJ with all non-privileged information about individuals responsible for misconduct, including the highest and lowest level employees and officials, in order to receive cooperation credit.[7] Then in 2022, DAG Monaco announced further updates further reinforcing the DOJ's commitment to individual responsibility for corporate crimes, including updated considerations for evaluating a company's compliance program.[8] The 2022 Monaco Memo previews expectations later embellished in the DOJ's 2023 Guidance, including a focus on compensation incentives and related considerations of when to require independent compliance monitoring.

> "It all comes back to corporate culture…"
> - Deputy Attorney General Lisa O. Monaco
> September 15, 2022

[7] Monaco, Lisa O., "Corporate Crime Advisory Group and Initial Revisions to Corporate Criminal Enforcement Policies" (October 28, 2021) available at https://www.justice.gov/dag/page/file/1445106/download.

[8] Monaco, Lisa O., "Further Revisions to Corporate Criminal Enforcement Policies" (September 15, 2022). The 2022 Monaco Memo also emphasizes that the company disclosure must be "timely" and focus on producing the most relevant evidence of criminality. Further, companies must timely preserve, collect and disclose relevant information in order to get full cooperation credit. The memo also focuses on the DOJ evaluating a company's entire history of misconduct, including criminal, civil and regulatory matters, when making decisions about how to resolve an investigation.

DOJ's 2023 "Evaluation of Corporate Compliance Programs"

The DOJ issued its updated **"Evaluation of Corporate Compliance Programs (Updated March 2023)" [TAB 4] (2023 Guidance),** adding significant new considerations as compared to the 2020 Guidance. A handy **redline** comparing the 2020 to the 2023 version is attached at **[TAB 5]**. For example, the measure of whether a compliance program is effective depends on not only whether it is designed to detect misconduct, but also whether it is designed to **prevent** misconduct. Other additions to the 2020 Guidance include:

- An assessment of whether corporations use nondisclosure agreements to inhibit public disclosure of wrongdoing.
- Attention to messaging platforms and personal device use policies: what channels are allowed and why; what policies/procedures and enforcement; risk management, data security.
- An entirely new section, "Independence and Empowerment," which focuses on the incentives and independence of the compliance function, asking:
    - "Is compensation for employees who are responsible for investigating and adjudicating misconduct structured in a way that ensures the compliance team is empowered to enforce the policies and ethical values of the company?"
    - "Who determines the compensation, including bonuses, as well as discipline and promotion of compliance personnel or others within the organization that have a role in the disciplinary process generally?"
- Another new section on overall "Compensation Structures and Consequence Management (CM)":
    - Metrics to ensure consistency in discipline.
    - Suggesting the companies "publiciz[e] disciplinary actions internally, where appropriate…" and asking in the case of executive exits: "are the actual reasons for discipline communicated to employees in all cases? If not, why not?"
    - Tracking data to measure effectiveness of investigations and CM: the number of substantiated cases, average time to completion, effectiveness and consistency of disciplinary measures across levels, geography, business units/departments.
    - Whether the compliance program uses compensation to incentivize compliance and uses financial incentives to mitigate misconduct such as compensation clawback provisions, the escrowing of compensation or financial penalties for misconduct.
    - Financial incentive tools may include affirmative metrics and benchmarks to reward.
    - Compliance-promoting behavior, promotions, bonuses, opportunities to serve as a compliance "champion" and "make compliance a significant metric for management bonuses."

In sum, the 2020 and 2023 DOJ Guidance are a robust resource and blueprint for the design, implementation, maintenance and ongoing monitoring and auditing of an effective compliance program.

A Final Note: On Self-Disclosure

The question of "when" to self-disclose misconduct is critical but subject to different approaches. In January 2023 the DOJ published the Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy (which previously only applied to Foreign Corrupt Practices Act (FCPA) cases but which now applies to all DOJ corporate criminal matters). This updated policy indicates that that a declination is available only if "voluntary self-disclosure was made **immediately upon the company becoming aware of the allegation of misconduct**." By contrast, the DOJ Civil Division, Consumer Protection Branch, in its updated February 2023 protocol, requires disclosure "prior to an imminent threat" or "**within a reasonably prompt time after becoming aware of the offense**." HHS OIG's 2021 disclosure protocol states that companies are expected to conduct an internal investigation and report findings to the OIG and must complete the investigation at latest 90 days after its initial disclosure submission as well as ensure that the violative conduct has ended or that the improper arrangement will be terminated within 90 days of submission.

Meanwhile, the health-care-industry-specific 2023 GCPG takes a different approach that expressly gives companies more time to assess the matter before self-reporting:

> As a general matter, if credible evidence of misconduct from any source is discovered and, **after a reasonable inquiry**, the compliance officer or counsel has reason to believe that the misconduct may violate criminal, civil, or administrative law, then the entity should **promptly (not more than 60 days after the determination that credible evidence of a violation exists)** notify the appropriate Government authority of the misconduct. (2023 GCPG, at 61).

However, the 2023 GCPG also states that some violations "may be so serious that they warrant immediate notification to governmental authorities, prior to, or simultaneous with, commencing an internal investigation." Examples mentioned are acts that are "a clear violation of criminal law." However, companies need to be mindful that many potential violations of the Food, Drug & Cosmetic Act and Medicare program statutes, regulations and rules carry criminal penalties. Other factors to consider when potentially "immediately" reporting include a "significant adverse effect on either patient safety or the quality of care," or acts that "indicat[e] evidence of a systemic failure to comply with applicable laws, an existing CIA, or other standards of conduct, regardless of the financial impact on Federal health care." (2023 GCPG, at 61). Both of those exceptions clearly require companies to make a case-by-case assessment of the totality of the facts and legal issues at stake.

HHS OIG's 2003 Compliance Program Guidance for Pharmaceutical Manufacturers

Dated: April 18, 2003.
Elizabeth M. Duke,
Administrator.
[FR Doc. 03–10934 Filed 5–2–03; 8:45 am]
BILLING CODE 4165–15–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of Inspector General

OIG Compliance Program Guidance for Pharmaceutical Manufacturers

AGENCY: Office of Inspector General (OIG), HHS.

ACTION: Notice

SUMMARY: This **Federal Register** notice sets forth the recently issued Compliance Program Guidance for Pharmaceutical Manufacturers developed by the Office of Inspector General (OIG). Through this notice, the OIG is setting forth its general views on the value and fundamental principles of compliance programs for pharmaceutical manufacturers and the specific elements that pharmaceutical manufacturers should consider when developing and implementing an effective compliance program.

FOR FURTHER INFORMATION CONTACT: Mary E. Riordan or Nicole C. Hall, Office of Counsel to the Inspector General, (202) 619–2078.

SUPPLEMENTARY INFORMATION:

Background

Compliance program guidance is a major initiative of the OIG in its effort to engage the health care community in preventing and reducing fraud and abuse in federal health care programs. The purpose of the compliance program guidance is to encourage the use of internal controls to efficiently monitor adherence to applicable statutes, regulations and program requirements. In the last several years, the OIG has developed and issued compliance program guidance directed at the following segments of the health care industry: the hospital industry; home health agencies; clinical laboratories; third-party medical billing companies; the durable medical equipment, prosthetics, orthotics and supply industry; Medicare+Choice organizations offering coordinated care plans; hospices; nursing facilities; individual and small group physician practices; and ambulance suppliers.

Copies of these compliance program guidances can be found on the OIG Web site at *http://oig.hhs.gov/fraud/complianceguidance.html.*

Developing the Compliance Program Guidance for Pharmaceutical Manufacturers

On June 11, 2001, the OIG published a solicitation notice seeking information and recommendations for developing compliance program guidance for the pharmaceutical industry (66 FR 31246). In response to that solicitation notice, the OIG received eight comments from various outside sources. We carefully considered those comments, as well as previous OIG publications, such as other compliance program guidances and Special Fraud Alerts. In addition, we have taken into account past and ongoing fraud investigations conducted by the OIG's Office of Investigations and the Department of Justice, and have consulted with the Centers for Medicare and Medicaid Services (CMS) (formerly known as the Health Care Financing Administration). In an effort to ensure that all parties had a reasonable opportunity to provide input into a final product, draft compliance program guidance for the pharmaceutical industry was published in the **Federal Register** on October 3, 2002 (67 FR 62057) for further comments and recommendations.

Elements for an Effective Compliance Program

This compliance program guidance for pharmaceutical manufacturers contains seven elements that have been widely recognized as fundamental to an effective compliance program:

- Implementing written policies and procedures;
- Designating a compliance officer and compliance committee;
- Conducting effective training and education;
- Developing effective lines of communication;
- Conducting internal monitoring and auditing;
- Enforcing standards through well-publicized disciplinary guidelines; and
- Responding promptly to detected problems and undertaking corrective action.

These elements are included in previous guidances issued by the OIG. As with previously issued guidances, this compliance program guidance represents the OIG's suggestions on how pharmaceutical manufacturers can establish internal controls to ensure adherence to applicable rules and program requirements. The contents of this guidance should not be viewed as mandatory or as an exclusive discussion of the advisable elements of a compliance program. The document is intended to present voluntary guidance to the industry and not to represent binding standards for pharmaceutical manufacturers.

Office of Inspector General's Compliance Program Guidance for Pharmaceutical Manufacturers

I. Introduction

The Office of Inspector General (OIG) of the Department of Health and Human Services is continuing in its efforts to promote voluntary compliance programs for the health care industry. This compliance guidance is intended to assist companies that develop, manufacture, market, and sell pharmaceutical drugs or biological products (pharmaceutical manufacturers) in developing and implementing internal controls and procedures that promote adherence to applicable statutes, regulations, and requirements of the federal health care programs[1] and in evaluating and, as necessary, refining existing compliance programs.

This guidance provides the OIG's views on the fundamental elements of pharmaceutical manufacturer compliance programs and principles that each pharmaceutical manufacturer should consider when creating and implementing an effective compliance program. This guide is not a compliance program. Rather, it is a set of guidelines that pharmaceutical manufacturers should consider when developing and implementing a compliance program or evaluating an existing one. For those manufacturers with an existing compliance program, this guidance may serve as a benchmark or comparison against which to measure ongoing efforts.

A pharmaceutical manufacturer's implementation of an effective compliance program may require a significant commitment of time and resources by various segments of the organization. In order for a compliance program to be effective, it must have the support and commitment of senior management and the company's governing body. In turn, the corporate leadership should strive to foster a culture that promotes the prevention, detection, and resolution of instances of problems. Although an effective compliance program may require a reallocation of existing resources, the long-term benefits of establishing a compliance program significantly outweigh the initial costs.

In a continuing effort to collaborate closely with the pharmaceutical industry, the OIG published a notice in

[1] (Endnotes appear at end of document)

the **Federal Register** soliciting comments and recommendations on what should be included in this compliance program guidance.[2] Following our review of comments received in response to the solicitation notice, we published draft compliance guidance in the **Federal Register** in order to solicit further comments and recommendations.[3] In addition to considering the comments received in response to that solicitation notice and the draft compliance guidance, in finalizing this guidance we reviewed previous OIG publications, including OIG advisory opinions, safe harbor regulations (including the preambles) relating to the federal anti-kickback statute,[4] Special Fraud Alerts, as well as reports issued by the OIG's Office of Audit Services and Office of Evaluation and Inspections relevant to the pharmaceutical industry. (These materials are available on the OIG Web page at *http://oig.hhs.gov.*) In addition, we relied on the experience gained from investigations of pharmaceutical manufacturers conducted by OIG's Office of Investigations, the Department of Justice, and the state Medicaid Fraud Control Units. We also held meetings with four groups of industry stakeholders—Pharmaceutical Research and Manufacturers of America (PhRMA) and pharmaceutical manufacturer representatives; health plan and health plan association representatives; representatives of pharmacy benefit managers (PBMs) and representatives of the American Medical Association (AMA) and its member organizations.

A. Benefits of a Compliance Program

The OIG believes a comprehensive compliance program provides a mechanism that addresses the public and private sectors' mutual goals of reducing fraud and abuse; enhancing health care provider operational functions; improving the quality of health care services; and reducing the cost of health care. Attaining these goals provides positive results to the pharmaceutical manufacturer, the government, and individual citizens alike. In addition to fulfilling its legal duty to avoid submitting false or inaccurate pricing or rebate information to any federal health care program or engaging in illegal marketing activities, a pharmaceutical manufacturer may gain important additional benefits by voluntarily implementing a compliance program. The benefits may include:

- A concrete demonstration to employees and the community at large of the company's commitment to honest and responsible corporate conduct;
- An increased likelihood of preventing, or at least identifying, and correcting unlawful and unethical behavior at an early stage;
- A mechanism to encourage employees to report potential problems and allow for appropriate internal inquiry and corrective action; and
- Through early detection and reporting, minimizing any financial loss to the government and any corresponding financial loss to the company.

The OIG recognizes that the implementation of a compliance program may not entirely eliminate improper conduct from the operations of a pharmaceutical manufacturer. However, a good faith effort by the company to comply with applicable statutes and regulations as well as federal health care program requirements, demonstrated by an effective compliance program, significantly reduces the risk of unlawful conduct and any penalties that result from such behavior.

B. Application of Compliance Program Guidance

Given the wide diversity within the pharmaceutical industry, there is no single "best" pharmaceutical manufacturer compliance program. The OIG recognizes the complexities of this industry and the differences among industry members. Some pharmaceutical manufacturers are small and may have limited resources to devote to compliance measures. Conversely, other companies are well-established, large multi-national corporations with a widely dispersed work force. Some companies may have well-developed compliance programs already in place; others only now may be initiating such efforts. The OIG also recognizes that pharmaceutical manufacturers are subject to extensive regulatory requirements in addition to fraud and abuse-related issues and that many pharmaceutical manufacturers have addressed these obligations through compliance programs. Accordingly, the OIG strongly encourages pharmaceutical manufactures to develop and implement or refine (as necessary) compliance elements that uniquely address the areas of potential problems, common concern, or high risk that apply to their own companies (or, as applicable, to the U.S. operations of their companies).

For example, although they are not exhaustive of all potential risk areas, the OIG has identified three major potential risk areas for pharmaceutical manufacturers: (1) Integrity of data used by state and federal governments to establish payment; (2) kickbacks and other illegal remuneration; and (3) compliance with laws regulating drug samples. The risk areas are discussed in greater detail in section II.B.2. below. The compliance measures adopted by a pharmaceutical manufacturer should be tailored to fit the unique environment of the company (including its organizational structure, operations and resources, as well as prior enforcement experience). In short, the OIG recommends that each pharmaceutical manufacturer should adapt the objectives and principles underlying the measures outlined in this guidance to its own particular circumstances.[5]

II. Compliance Program Elements

A. The Basic Compliance Elements

The OIG believes that every effective compliance program must begin with a formal commitment by the pharmaceutical manufacturer's board of directors or other governing body. Evidence of that commitment should include the allocation of adequate resources, a timetable for the implementation of the compliance measures, and the identification of an individual to serve as a compliance officer to ensure that each of the recommended and adopted elements is addressed. Once a commitment has been undertaken, a compliance officer should immediately be chosen to oversee the implementation of the compliance program.

The elements listed below provide a comprehensive and firm foundation upon which an effective compliance program may be built. Further, they are likely to foster the development of a corporate culture of compliance. The OIG recognizes that full implementation of all elements may not be immediately feasible for all pharmaceutical manufacturers. However, as a first step, a good faith and meaningful commitment on the part of the company's management will substantially contribute to the program's successful implementation. As the compliance program is implemented, that commitment should filter down through management to every employee and contractor of the pharmaceutical manufacturer, as applicable for the particular individual.

At a minimum, a comprehensive compliance program should include the following elements:

(1) The development and distribution of written standards of conduct, as well as written policies, procedures and protocols that verbalize the company's commitment to compliance (*e.g.*, by including adherence to the compliance

program as an element in evaluating management and employees) and address specific areas of potential fraud and abuse, such as the reporting of pricing and rebate information to the federal health care programs, and sales and marketing practices;

(2) The designation of a compliance officer and other appropriate bodies (*e.g.*, a corporate compliance committee) charged with the responsibility for developing, operating, and monitoring the compliance program, and with authority to report directly to the board of directors and/or the president or CEO;

(3) The development and implementation of regular, effective education and training programs for all affected employees;

(4) The creation and maintenance of an effective line of communication between the compliance officer and all employees, including a process (such as a hotline or other reporting system) to receive complaints or questions, and the adoption of procedures to protect the anonymity of complainants and to protect whistleblowers from retaliation;

(5) The use of audits and/or other risk evaluation techniques to monitor compliance, identify problem areas, and assist in the reduction of identified problems;

(6) The development of policies and procedures addressing the non-employment or retention of individuals or entities excluded from participation in federal health care programs, and the enforcement of appropriate disciplinary action against employees or contractors who have violated company policies and procedures and/or applicable federal health care program requirements; and

(7) The development of policies and procedures for the investigation of identified instances of noncompliance or misconduct. These should include directions regarding the prompt and proper response to detected offenses, such as the initiation of appropriate corrective action and preventive measures and processes to report the offense to relevant authorities in appropriate circumstances.

B. Written Policies and Procedures

In developing a compliance program, every pharmaceutical manufacturer should develop and distribute written compliance standards, procedures, and practices that guide the company and the conduct of its employees in day-to-day operations. These policies and procedures should be developed under the direction and supervision of the compliance officer, the compliance committee, and operational managers. At a minimum, the policies and procedures should be provided to all employees who are affected by these policies, and to any agents or contractors who may furnish services that impact federal health care programs (*e.g.*, contractors involved in the co-promotion of a manufacturer's products).

1. Code of Conduct

Although a clear statement of detailed and substantive policies and procedures is at the core of a compliance program, the OIG recommends that pharmaceutical manufacturers also develop a general corporate statement of ethical and compliance principles that will guide the company's operations. One common expression of this statement of principles is the code of conduct. The code should function in the same fashion as a constitution, *i.e.*, as a document that details the fundamental principles, values, and framework for action within an organization. The code of conduct for a pharmaceutical manufacturer should articulate the company's expectations of commitment to compliance by management, employees, and agents, and should summarize the broad ethical and legal principles under which the company must operate. Unlike the more detailed policies and procedures, the code of conduct should be brief, easily readable, and cover general principles applicable to all employees.

As appropriate, the OIG strongly encourages the participation and involvement of the pharmaceutical manufacturer's board of directors, CEO, president, members of senior management, and other personnel from various levels of the organizational structure in the development of all aspects of the compliance program, especially the code of conduct. Management and employee involvement in this process communicates a strong and explicit commitment by management to foster compliance with applicable federal health care program requirements. It also communicates the need for all employees to comply with the organization's code of conduct and policies and procedures.

2. Specific Risk Areas

This section is intended to help prudent pharmaceutical manufacturers identify areas of their operations that present potential risk of liability under several key federal fraud and abuse statutes and regulations.[6] This section focuses on areas that are currently of concern to the enforcement community and is not intended to address all potential risk areas for pharmaceutical manufacturers. Importantly, the identification of a particular practice or activity in this section is not intended to imply that the practice or activity is necessarily illegal in all circumstances or that it may not have a valid or lawful purpose underlying it.

This section addresses the following areas of significant concern for pharmaceutical manufacturers: (1) Integrity of data used by state and federal governments to establish payment amounts; (2) kickbacks and other illegal remuneration; and (3) compliance with laws regulating drug samples.

This guidance does not create any new law or legal obligations, and the discussions that follow are not intended to present detailed or comprehensive summaries of lawful and unlawful activity. Rather, these discussions should be used as a starting point for a manufacturer's legal review of its particular practices and for development of policies and procedures to reduce or eliminate potential risk.

a. Integrity of Data Used To Establish or Determine Government Reimbursement. Many federal and state health care programs establish or ultimately determine reimbursement rates for pharmaceuticals, either prospectively or retrospectively, using price and sales data directly or indirectly furnished by pharmaceutical manufacturers. The government sets reimbursement with the expectation that the data provided are complete and accurate. The knowing submission of false, fraudulent, or misleading information is actionable. A pharmaceutical manufacturer may be liable under the False Claims Act[7] if government reimbursement (including, but not limited to, reimbursement by Medicare and Medicaid) for the manufacturer's product depends, in whole or in part, on information generated or reported by the manufacturer, directly or indirectly, and the manufacturer has knowingly (as defined in the False Claims Act) failed to generate or report such information completely and accurately. Manufacturers may also be liable for civil money penalties under various laws, rules and regulations. Moreover, in some circumstances, inaccurate or incomplete reporting may be probative of liability under the federal anti-kickback statute.

Where appropriate, manufacturers' reported prices should accurately take into account price reductions, cash discounts, free goods contingent on a purchase agreement, rebates, up-front payments, coupons, goods in kind, free or reduced-price services, grants, or

other price concessions or similar benefits offered to some or all purchasers. Any discount, price concession, or similar benefit offered on purchases of multiple products should be fairly apportioned among the products (and could potentially raise anti-kickback issues). Underlying assumptions used in connection with reported prices should be reasoned, consistent, and appropriately documented, and pharmaceutical manufacturers should retain all relevant records reflecting reported prices and efforts to comply with federal health care program requirements.

Given the importance of the Medicaid Rebate Program, as well as other programs that rely on Medicaid Rebate Program benchmarks (such as the 340B Program [8]), manufacturers should pay particular attention to ensuring that they are calculating Average Manufacturer Price and Best Price accurately and that they are paying appropriate rebate amounts for their drugs.[9]

In sum, pharmaceutical manufacturers are responsible for ensuring the integrity of data they generate that is used for government reimbursement purposes.

b. Kickbacks and Other Illegal Remuneration—*A. General Considerations.* Pharmaceutical manufacturers, as well as their employees and agents, should be aware of the federal anti-kickback statute and the constraints it places on the marketing and promotion of products reimbursable by the federal health care programs, including, but not limited to, Medicare and Medicaid. In the health care sector, many common business activities, including, for example, sales, marketing, discounting, and purchaser relations, potentially implicate the anti-kickback statute. Pharmaceutical manufacturers and their employees and agents should be aware that the anti-kickback statute prohibits in the health care industry some practices that are common in other business sectors. In short, practices that may be common or longstanding in other businesses are not necessarily acceptable or lawful when soliciting federal health care program business.

The anti-kickback statute is a criminal prohibition against payments (in any form, whether the payments are direct or indirect) made purposefully to induce or reward the referral or generation of federal health care business. The anti-kickback statute addresses not only the offer or payment of anything of value for patient referrals, but also the offer or payment of anything of value in return for purchasing, leasing, ordering, or arranging for or recommending the purchase, lease, or ordering of any item or service reimbursable in whole or part by a federal health care program. The statute extends equally to the solicitation or acceptance of remuneration for referrals. Liability under the anti-kickback statute is determined separately for each party involved. In addition to criminal penalties, violators may be subject to civil monetary sanctions and exclusion from the federal health care programs. Under certain circumstances, a violation of the anti-kickback statute may give rise to liability under the False Claims Act.

Although liability under the anti-kickback statute ultimately turns on a party's intent, it is possible to identify arrangements or practices that may present a significant potential for abuse. Initially, a manufacturer should identify any remunerative relationship between itself (or its representatives) and persons or entities in a position to generate federal health care business for the manufacturer directly or indirectly. Persons or entities in a position to generate federal health care business include, for example, purchasers, benefit managers, formulary committee members, group purchasing organizations (GPOs), physicians and certain allied health care professionals, and pharmacists. The next step is to determine whether any *one* purpose of the remuneration may be to induce or reward the referral or recommendation of business payable in whole or in part by a Federal health care program. Importantly, a lawful purpose will not legitimize a payment that also has an unlawful purpose.

Although any arrangement satisfying both tests requires careful scrutiny from a manufacturer, the courts have identified several potentially aggravating considerations that can be useful in identifying arrangements at greatest risk of prosecution. In particular, manufacturers should ask the following questions, among others, about any problematic arrangements or practices they identify:

- Does the arrangement or practice have a potential to interfere with, or skew, clinical decision-making? Does it have a potential to undermine the clinical integrity of a formulary process? If the arrangement or practice involves providing information to decision-makers, prescribers, or patients, is the information complete, accurate, and not misleading?
- Does the arrangement or practice have a potential to increase costs to the federal health care programs, beneficiaries, or enrollees? Does the arrangement or practice have the potential to be a disguised discount to circumvent the Medicaid Rebate Program Best Price calculation?
- Does the arrangement or practice have a potential to increase the risk of overutilization or inappropriate utilization?
- Does the arrangement or practice raise patient safety or quality of care concerns?

Manufacturers that have identified problematic arrangements or practices can take a number of steps to reduce or eliminate the risk of an anti-kickback violation. Detailed guidance relating to a number of specific practices is available from several sources. Most importantly, the anti-kickback statute and the corresponding regulations establish a number of "safe harbors" for common business arrangements, including personal services and management contracts, 42 CFR 1001.952(d), warranties, 42 CFR 1001.952(g), discounts, 42 CFR 1001.952(h), employment, 42 CFR 1001.952(i), GPOs, 42 CFR 1001.952(j), and certain managed care and risk sharing arrangements, 42 CFR 1001.952(m), (t), and (u). *Safe harbor protection requires strict compliance with all applicable conditions set out in the relevant safe harbor.* Although compliance with a safe harbor is voluntary and failure to comply with a safe harbor does not mean an arrangement is illegal, many arrangements can be structured to fit in safe harbors, and we recommend that pharmaceutical manufacturers structure arrangements to fit in a safe harbor whenever possible. Other available guidance includes special fraud alerts and advisory bulletins issued by the OIG identifying and discussing particular practices or issues of concern and OIG advisory opinions issued to specific parties about their particular business arrangements. Parties may apply for an OIG advisory opinion using the procedures set out at 42 CFR part 1008. The safe harbor regulations (and accompanying **Federal Register** preambles), fraud alerts and bulletins, advisory opinions (and instructions for obtaining them), and other guidance are available on the OIG web site at *http://oig.hhs.gov.*

B. Key Areas of Potential Risk. The following discussion highlights several known areas of potential risk. The propriety of any particular arrangement can only be determined after a detailed examination of the attendant facts and circumstances. *The identification of a given practice or activity as "suspect" or as an area of "risk" does not mean it is necessarily illegal or unlawful, or that it*

cannot be properly structured to fit in a safe harbor. Nor does it mean that the practice or activity is not beneficial from a clinical, cost, or other perspective. Rather, the areas identified below are those areas of activity that have a potential for abuse based on historical law enforcement experience and that should receive close scrutiny from manufacturers. The discussion highlights potential risks under the anti-kickback statute arising from pharmaceutical manufacturers' relationships with three groups: purchasers (including those using formularies) and their agents; persons and entities in a position to make or influence referrals (including physicians and other health care professionals); and sales agents.

(1) Relationships with Purchasers and their Agents—(a) Discounts and Other Remuneration to Purchasers. Pharmaceutical manufacturers offer purchasers a variety of price concessions and other remuneration to induce the purchase of their products. Purchasers include direct purchasers (*e.g.,* hospitals, nursing homes, pharmacies, some physicians), as well as indirect purchasers (*e.g.,* health plans). Inducements offered to purchasers potentially implicate the anti-kickback statute if the purchased products are reimbursable to the purchasers, in whole or in part, directly or indirectly, by any of the federal health care programs. Any remuneration from a manufacturer provided to a purchaser that is expressly or impliedly related to a sale potentially implicates the anti-kickback statute and should be carefully reviewed.

Discounting arrangements are prevalent in the pharmaceutical industry and deserve careful scrutiny particularly because of their potential to implicate the Best Price requirements of the Medicaid Rebate Program. Because the Medicaid Rebate Program in many instances requires that states receive rebates based on the Best Price offered by a pharmaceutical manufacturer to other purchasers, manufacturers have a strong financial incentive to hide *de facto* pricing concessions to other purchasers to avoid passing on the same discount to the states. Because of the potential direct and substantial effect of such practices on federal health care program expenditures and the interest of some manufacturers in avoiding price concessions that would trigger rebates to the states, any remuneration from a manufacturer to a purchaser, however characterized, should be carefully scrutinized.

Discounts. Public policy favors open and legitimate price competition in health care. Thus, the anti-kickback statute contains an exception for discounts offered to customers that submit claims to the federal health care programs, if the discounts are properly disclosed and accurately reported. *See* 42 U.S.C. 1320a–7b(b)(3)(A); 42 CFR 1001.952(h). However, to qualify for the exception, the discount must be in the form of a *reduction in the price* of the good or service based on an arms-length transaction. In other words, the exception covers only reductions in the product's price. Moreover, the regulations provide that the discount must be given at the time of sale or, in certain cases, set at the time of sale, even if finally determined subsequent to the time of sale (*i.e.*, a rebate).

Manufacturers offering discounts should thoroughly familiarize themselves, and have their sales and marketing personnel familiarize themselves, with the discount safe harbor at 42 CFR 1001.952(h) (and, if relevant, the safe harbors for price reductions in the managed care context, 42 CFR 1001.952(m), (t), and (u)). In particular, manufacturers should pay attention to the discount safe harbor requirements applicable to "sellers" and "offerors" of discounts. Under the safe harbor, sellers and offerors have specific obligations that include (i) informing a customer of any discount and of the customer's reporting obligations with respect to that discount, and (ii) refraining from any action that would impede a customer's ability to comply with the safe harbor. To fulfill the safe harbor requirements, manufacturers will need to know how their customers submit claims to the federal health care programs (*e.g.,* whether the customer is a managed care, cost-based, or charge-based biller). Compliance with the safe harbor is determined separately for each party.

Product Support Services. Pharmaceutical manufacturers sometimes offer purchasers certain support services in connection with the sale of their products. These services may include billing assistance tailored to the purchased products, reimbursement consultation, and other programs specifically tied to support of the purchased product. Standing alone, services that have no substantial independent value to the purchaser may not implicate the anti-kickback statute. However, if a manufacturer provides a service having no independent value (such as limited reimbursement support services in connection with its own products) in tandem with another service or program that confers a benefit on a referring provider (such as a reimbursement guarantee that eliminates normal financial risks), the arrangement would raise kickback concerns. For example, the anti-kickback statute would be implicated if a manufacturer were to couple a reimbursement support service with a promise that a purchaser will pay for ordered products only if the purchaser is reimbursed by a federal health care program.

Educational Grants. Pharmaceutical manufacturers sometimes provide grant funding for a wide range of educational activities. While educational funding can provide valuable information to the medical and health care industry, manufacturer grants to purchasers, GPOs, PBMs and similar entities raise concerns under the anti-kickback statute. Funding that is conditioned, in whole or in part, on the purchase of product implicates the statute, even if the educational or research purpose is legitimate. Furthermore, to the extent the manufacturer has any influence over the substance of an educational program or the presenter, there is a risk that the educational program may be used for inappropriate marketing purposes.

To reduce the risks that a grant program is used improperly to induce or reward product purchases or to market product inappropriately, manufacturers should separate their grant making functions from their sales and marketing functions. Effective separation of these functions will help insure that grant funding is not inappropriately influenced by sales or marketing motivations and that the educational purposes of the grant are legitimate. Manufacturers should establish objective criteria for making grants that do not take into account the volume or value of purchases made by, or anticipated from, the grant recipient and that serve to ensure that the funded activities are *bona fide.* The manufacturer should have no control over the speaker or content of the educational presentation. Compliance with such procedures should be documented and regularly monitored.

Research Funding. Manufacturers often contract with purchasers of their products to conduct research activities on behalf of the manufacturer on a fee-for-service basis. These contracts should be structured to fit in the personal services safe harbor whenever possible. Payments for research services should be fair market value for legitimate, reasonable, and necessary services. Post-marketing research activities should be especially scrutinized to ensure that they are legitimate and not simply a pretext to generate prescriptions of a drug. Prudent manufacturers will develop contracting procedures that

clearly separate the awarding of research contracts from marketing. Research contracts that originate through the sales or marketing functions—or that are offered to purchasers in connection with sales contacts—are particularly suspect.

Pharmaceutical manufacturers sometimes provide funding to their purchasers for use in the purchasers' own research. In many cases, the research provides valuable scientific and clinical information, improves clinical care, leads to promising new treatments, promotes better delivery of health care, or otherwise benefits patients. However, as with educational grants, if linked directly or indirectly to the purchase of product, research grants can be misused to induce the purchase of business without triggering Medicaid Best Price obligations. To reduce risk, manufacturers should insulate research grant making from sales and marketing influences.

Other remuneration to purchasers. As already noted, any remuneration from a manufacturer provided to a purchaser that is expressly or impliedly related to a sale potentially implicates the anti-kickback statute and should be carefully reviewed. Examples of remuneration in connection with a sale include, but are not limited to, "prebates" and "upfront payments," other free or reduced-price goods or services, and payments to cover the costs of "converting" from a competitor's product. Selective offers of remuneration (*i.e.*, offers made to some but not all purchasers) may increase potential risk if the selection criteria relate directly or indirectly to the volume or value of business generated. In addition, manufacturers may contract with purchasers to provide services to the manufacturer, such as data collection services. These contracts should be structured whenever possible to fit in the personal services safe harbor; in all cases, the remuneration should be fair market value for legitimate, reasonable, and necessary services.

(b) Formularies and Formulary Support Activities. To help control drug costs while maintaining clinical appropriateness and quality of patient care, many purchasers of pharmaceutical products, including indirect purchasers such as health plans, have developed drug formularies to promote rational, clinically appropriate, safe, and cost-effective drug therapy. Formularies are a well-established tool for the effective management of drug benefits. The formulary development process—typically overseen by a committee of physicians, pharmacists, and other health care professionals—determines the drugs that are covered and, if tiered benefit levels are utilized, to which tier the drugs are assigned. So long as the determination of clinical efficacy and appropriateness of formulary drugs by the formulary committee precedes, and is paramount to, the consideration of costs, the development of a formulary is unlikely to raise significant issues under the anti-kickback statute.

Formulary support activities, including related communications with patients and physicians to encourage compliance, are an integral and essential component of successful pharmacy benefits management. Proper utilization of a formulary maximizes the cost-effectiveness of the benefit and assures the quality and appropriateness of the drug therapy. When provided by a PBM, these services are part of the PBM's formulary and benefit management function—a service provided to its customers—and markedly different from its purchasing agent/price negotiator role. Most importantly, the benefits of these formulary support activities inure directly to the PBM and its customers through lower costs.

To date, Medicare and Medicaid involvement with outpatient drug formularies has been limited primarily to Medicaid and Medicare managed care plans. In light of the safe harbors under the anti-kickback statute for those managed care arrangements, the financial arrangements between health plans and pharmaceutical manufacturers or, where the pharmacy benefit is managed by a PBM, the arrangements among the three parties, have received relatively little scrutiny. However, as federal program expenditures for, and coverage of, outpatient pharmaceuticals increase, scrutiny under the anti-kickback statute has also increased. Several practices appear to have the potential for abuse.

- *Relationships with formulary committee members.* Given the importance of formulary placement for a manufacturer's products, unscrupulous manufacturers and sales representatives may attempt to influence committee deliberations. Any remuneration from a manufacturer or its agents directly or indirectly to person in a position to influence formulary decisions related to the manufacturer's products are suspect and should be carefully scrutinized. Manufacturers should also review their contacts with sponsors of formularies to ensure that price negotiations do not influence decisions on clinical safety or efficacy.
- *Payments to PBMs.* Any rebates or other payments by drug manufacturers to PBMs that are based on, or otherwise related to, the PBM's customers' purchases *potentially* implicate the anti-kickback statute. Protection is available by structuring such arrangements to fit in the GPO safe harbor at 42 CFR 1001.952(j). That safe harbor requires, among other things, that the payments be authorized in advance by the PBM's customer and that all amounts actually paid to the PBM on account of the customer's purchases be disclosed in writing at least annually to the customer. In addition, arrangements with PBMs that assume risk may raise different issues; depending on the circumstances, protection for such arrangements may be available under the managed care safe harbors at 42 CFR 1001.952(m), (t) and (u).
- *Formulary placement payments.* Lump sum payments for inclusion in a formulary or for exclusive or restricted formulary status are problematic and should be carefully scrutinized.

In addition, some manufacturers provide funding for purchasers' or PBMs' formulary support activities, especially communications with physicians and patients. While the communications may indirectly benefit the manufacturer, the primary economic beneficiary is typically the formulary sponsor. In other words, the manufacturer's dollars appear to replace dollars that would or should be spent by the sponsor. To the extent the manufacturers' payments are linked to drug purchases directly or indirectly, they potentially implicate the anti-kickback statute. Among the questions that should be examined by a manufacturer in connection with these activities are: Is the funding tied to specific drugs or categories? If so, are the categories especially competitive? Is the formulary sponsor funding similar activities for other drug categories? Has funding of PBM activities increased as rebates are increasingly passed back to PBM customers?

(c) Average Wholesale Price. The "spread" is the difference between the amount a customer pays for a product and the amount the customer receives upon resale of the product to the patient or other payer. In many situations under the federal programs, pharmaceutical manufacturers control not only the amount at which they sell a product to their customers, but also the amount those customers who purchase the product for their own accounts and thereafter bill the federal health care programs will be reimbursed. To the extent that a manufacturer controls the "spread," it controls its customer's profit.

Average Wholesale Price (AWP) is the benchmark often used to set reimbursement for prescription drugs under the Medicare Part B program. For covered drugs and biologicals, Medicare Part B generally reimburses at "95 percent of average wholesale price." 42 U.S.C. 1395u(o). Similarly many state Medicaid programs and other payers base reimbursement for drugs and biologicals on AWP. Generally, AWP or pricing information used by commercial price reporting services to determine AWP is reported by pharmaceutical manufacturers.

If a pharmaceutical manufacturer purposefully manipulates the AWP to increase its customers' profits by increasing the amount the federal health care programs reimburse its customers, the anti-kickback statute is implicated. Unlike *bona fide* discounts, which transfer remuneration from a seller to a buyer, manipulation of the AWP transfers remuneration to a seller's immediate customer from a subsequent purchaser (the federal or state government). Under the anti-kickback statute, offering remuneration to a purchaser or referral source is improper if one purpose is to induce the purchase or referral of program business. In other words, it is illegal for a manufacturer knowingly to establish or inappropriately maintain a particular AWP if one purpose is to manipulate the "spread" to induce customers to purchase its product.

In the light of this risk, we recommend that manufacturers review their AWP reporting practices and methodology to confirm that marketing considerations do not influence the process. Furthermore, manufacturers should review their marketing practices. The conjunction of manipulation of the AWP to induce customers to purchase a product with active marketing of the spread is strong evidence of the unlawful intent necessary to trigger the anti-kickback statute. Active marketing of the spread includes, for example, sales representatives promoting the spread as a reason to purchase the product or guaranteeing a certain profit or spread in exchange for the purchase of a product.

(2) Relationships with Physicians and Other Persons and Entities in a Position to Make or Influence Referrals. Pharmaceutical manufacturers and their agents may have a variety of remunerative relationships with persons or entities in a position to refer, order, or prescribe—or influence the referral, ordering, or prescribing of—the manufacturers' products, even though the persons or entities may not themselves purchase (or in the case of GPOs or PBMs, arrange for the purchase of) those products. These remunerative relationships potentially implicate the anti-kickback statute. The following discussion focuses on relationships with physicians, but the same principles would apply when evaluating relationships with other parties in a position to influence referrals, including, without limitation, pharmacists and other health care professionals.

Manufacturers, providers, and suppliers of health care products and services frequently cultivate relationships with physicians in a position to generate business for them through a variety of practices, including gifts, entertainment, and personal services compensation arrangements. These activities have a high potential for fraud and abuse and, historically, have generated a substantial number of anti-kickback convictions. There is no substantive difference between remuneration from a pharmaceutical manufacturer or from a durable medical equipment or other supplier—if the remuneration is intended to generate any federal health care business, it potentially violates the anti-kickback statute.

Any time a pharmaceutical manufacturer provides anything of value to a physician who might prescribe the manufacturer's product, the manufacturer should examine whether it is providing a valuable tangible benefit to the physician with the intent to induce or reward referrals. For example, if goods or services provided by the manufacturer eliminate an expense that the physician would have otherwise incurred (*i.e.*, have independent value to the physician), or if items or services are sold to a physician at less than their fair market value, the arrangement may be problematic if the arrangement is tied directly or indirectly to the generation of federal health care program business for the manufacturer. Moreover, under the anti-kickback statute, neither a legitimate purpose for an arrangement (*e.g.*, physician education), nor a fair market value payment, will necessarily protect remuneration if there is also an illegal purpose (*i.e.*, the purposeful inducement of business).

In light of the obvious risks inherent in these arrangements, whenever possible prudent manufacturers and their agents or representatives should structure relationships with physicians to fit in an available safe harbor, such as the safe harbors for personal services and management contracts, 42 CFR 1001.952(d), or employees, 42 CFR 1001.952(i). *An arrangement must fit squarely in a safe harbor to be protected.* In addition, arrangements that do not fit in a safe harbor should be reviewed in light of the totality of all facts and circumstances, bearing in mind the following factors, among others:

- *Nature of the relationship between the parties.* What degree of influence does the physician have, directly or indirectly, on the generation of business for the manufacturer? Does the manufacturer have other direct or indirect relationships with the physician or members of the physician's group?
- *Manner in which the remuneration is determined.* Does the remuneration take into account, directly or indirectly, the volume or value of business generated (*e.g.*, is the remuneration only given to persons who have prescribed or agreed to prescribe the manufacturer's product)? Is the remuneration conditioned in whole or in part on referrals or other business generated? Is there any service provided other than referrals?
- *Value of the remuneration.* Is the remuneration more than trivial in value, including all gifts to any individual, entity, or group of individuals? [10] Do fees for services exceed the fair market value of any legitimate, reasonable, and necessary services rendered by the physician to the manufacturer?
- *Potential federal program impact of the remuneration.* Does the remuneration have the potential to affect costs to any of the federal health care programs or their beneficiaries or to lead to overutilization or inappropriate utilization?
- *Potential conflicts of interest.* Would acceptance of the remuneration diminish, or appear to diminish, the objectivity of professional judgment? Are there patient safety or quality of care concerns? If the remuneration relates to the dissemination of information, is the information complete, accurate, and not misleading?

These concerns are addressed in the PhRMA Code on Interactions with Healthcare Professionals (the "PhRMA Code"), adopted on April 18, 2002, which provides useful and practical advice for reviewing and structuring these relationships. (The PhRMA Code is available through PhRMA's Web site at *http://www.phrma.org.*) Although compliance with the PhRMA Code will not protect a manufacturer as a matter of law under the anti-kickback statute, it will substantially reduce the risk of fraud and abuse and help demonstrate a good faith effort to comply with the applicable federal health care program requirements.

The following paragraphs discuss in greater detail several common or problematic relationships between manufacturers and physicians, including "switching" arrangements, consulting and advisory payments, payments for detailing, business courtesies and other gratuities, and educational and research activities.

• *Switching"* arrangements. As noted in the OIG's 1994 Special Fraud Alert (59 FR 65372; December 19, 1994), product conversion arrangements (also known as "switching" arrangements) are suspect under the anti-kickback statute. Switching arrangements involve pharmaceutical manufacturers offering physicians or others cash payments or other benefits each time a patient's prescription is changed to the manufacturer's product from a competing product. This activity clearly implicates the statute, and, while such programs may be permissible in certain managed care arrangements, manufacturers should review very carefully any marketing practices utilizing "switching" payments in connection with products reimbursable by federal health care programs.

Consulting and advisory payments. Pharmaceutical manufacturers frequently engage physicians and other health care professionals to furnish personal services as consultants or advisers to the manufacturer. In general, fair market value payments to small numbers of physicians for *bona fide* consulting or advisory services are unlikely to raise any significant concern. Compensating physicians as "consultants" when they are expected to attend meetings or conferences primarily in a passive capacity is suspect.

Also of concern are compensation relationships with physicians for services connected directly or indirectly to a manufacturer's marketing and sales activities, such as speaking, certain research, or preceptor or "shadowing" services. While these arrangements are potentially beneficial, they also pose a risk of fraud and abuse. In particular, the use of health care professionals for marketing purposes—including, for example, ghost-written papers or speeches—implicates the anti-kickback statute. While full disclosure by physicians of any potential conflicts of interest and of industry sponsorship or affiliation may reduce the risk of abuse, disclosure does not eliminate the risk.

At a minimum, manufacturers should periodically review arrangements for physicians' services to ensure that: (i) The arrangement is set out in writing; (ii) there is a legitimate need for the services; (iii) the services are provided; (iv) the compensation is at fair market value; and (v) all of the preceding facts are documented prior to payment. In addition, to further reduce their risk, manufacturers should structure services arrangements to comply with a safe harbor whenever possible.

Payments for detailing. Recently, some entities have been compensating physicians for time spent listening to sales representatives market pharmaceutical products. In some cases, these payments are characterized as "consulting" fees and may require physicians to complete minimal paperwork. Other companies pay physicians for time spent accessing web sites to view or listen to marketing information or perform "research." All of these activities are highly suspect under the anti-kickback statute, are highly susceptible to fraud and abuse, and should be strongly discouraged.

Business Courtesies and Other Gratuities. Pharmaceutical companies and their employees and agents often engage in a number of other arrangements that offer benefits, directly or indirectly, to physicians or others in a position to make or influence referrals. Examples of remunerative arrangements between pharmaceutical manufacturers (or their representatives) and parties in a position to influence referrals include:

• Entertainment, recreation, travel, meals, or other benefits in association with information or marketing presentations; and

• Gifts, gratuities, and other business courtesies.

As discussed above, these arrangements potentially implicate the anti-kickback statute if any one purpose of the arrangement is to generate business for the pharmaceutical company. While the determination of whether a particular arrangement violates the anti-kickback statute depends on the specific facts and circumstances, compliance with the PhRMA Code with respect to these arrangements should substantially reduce a manufacturer's risk.

Educational and Research Funding. In some cases, manufacturers contract with physicians to provide research services on a fee-for-service basis. These contracts should be structured to fit in the personal services safe harbor whenever possible. Payments for research services should be fair market value for legitimate, reasonable, and necessary services. Research contracts that originate through the sales or marketing functions—or that are offered to physicians in connection with sales contacts—are particularly suspect. Indicia of questionable research include, for example, research initiated or directed by marketers or sales agents; research that is not transmitted to, or reviewed by, a manufacturer's science component; research that is unnecessarily duplicative or is not needed by the manufacturer for any purpose other than the generation of business; and post-marketing research used as a pretense to promote product. Prudent manufacturers will develop contracting procedures that clearly separate the awarding of research contracts from marketing or promotion of their products.

In addition, pharmaceutical manufacturers also provide other funding for a wide range of physician educational and research activities. Manufacturers should review educational and research grants to physicians similarly to educational and research grants to purchasers (described above). As with grants to purchasers, the OIG recognizes that many grant-funded activities are legitimate and beneficial. When evaluating educational or research grants provided by manufacturers to physicians, manufacturers should determine if the funding is based, in any way, expressly or implicitly, on the physician's referral of the manufacturer's product. If so, the funding plainly implicates the anti-kickback statute. In addition, the manufacturer should determine whether the funding is for *bona fide* educational or research purposes. Absent unusual circumstances, grants or support for educational activities sponsored and organized by medical professional organizations raise little risk of fraud or abuse, provided that the grant or support is not restricted or conditioned with respect to content or faculty.

Pharmaceutical manufacturers often provide funding to other sponsors of continuing medical education (CME) programs. Manufacturers should take steps to ensure that neither they, nor their representatives, are using these activities to channel improper remuneration to physicians or others in a position to generate business for the manufacturer or to influence or control the content of the program.[11] In addition, manufacturers and sponsors of educational programs should be mindful of the relevant rules and regulations of the Food and Drug Administration. Codes of conduct promulgated by the CME industry may provide a useful starting point for manufacturers when reviewing their CME arrangements.

(3) Relationships with Sales Agents. In large part, a pharmaceutical manufacturer's commitment to an effective fraud and abuse compliance program can be measured by its

commitment to training and monitoring its sales force. A pharmaceutical manufacturer should: (i) Develop a regular and comprehensive training program for its sales force, including refresher and updated training on a regular basis, either in person or through newsletters, memoranda, or the like; (ii) familiarize its sales force with the minimum PhRMA Code standards and other relevant industry standards; (iii) institute and implement corrective action and disciplinary policies applicable to sales agents who engage in improper marketing; (iv) avail itself of the advisory opinion process if it has questions about particular practices used by its sales force; and (v) establish an effective system for tracking, compiling, and reviewing information about sales force activities, including, if appropriate, random spot checking.

In addition, manufacturers should carefully review their compensation arrangements with sales agents. Sales agents, whether employees or independent contractors, are paid to recommend and arrange for the purchase of the items or services they offer for sale on behalf of the pharmaceutical manufacturer they represent. Many arrangements can be structured to fit in the employment or personal services safe harbor. Arrangements that cannot fit into a safe harbor should be carefully reviewed. Among the factors that should be evaluated are:

- The amount of compensation;
- The identity of the sales agent engaged in the marketing or promotional activity (*e.g.*, is the agent a ''white coat'' marketer or otherwise in a position of exceptional influence);
- The sales agent's relationship with his or her audience;
- The nature of the marketing or promotional activity;
- The item or service being promoted or marketed; and
- The composition of the target audience.

Manufacturers should be aware that a compensation arrangement with a sales agent that fits in a safe harbor can still be evidence of a manufacturer's improper intent when evaluating the legality of the manufacturer's relationships with persons in a position to influence business for the manufacturer. For example, if a manufacturer provides sales employees with extraordinary incentive bonuses and expense accounts, there may well be an inference to be drawn that the manufacturer intentionally motivated the sales force to induce sales through lavish entertainment or other remuneration.

c. Drug Samples. The provision of drug samples is a widespread industry practice that can benefit patients, but can also be an area of potential risk to a pharmaceutical manufacturer. The Prescription Drug Marketing Act of 1987 (PDMA) governs the distribution of drug samples and forbids their sale. 21 U.S.C. 353(c)(1). A drug sample is defined to be a unit of the drug ''that is not intended to be sold * * * and is intended to promote the sale of the drug.'' 21 U.S.C. 353(c)(1). Failure to comply with the requirements of PDMA can result in sanctions. In some circumstances, if the samples have monetary value to the recipient (*e.g.*, a physician) and are used to treat federal health care program beneficiaries, the improper use of samples may also trigger liability under other statutes, including the False Claims Act and the anti-kickback statue.

Pharmaceutical manufacturers should closely follow the PDMA requirements (including all documentation requirements). In addition, manufacturers can minimize their risk of liability by: (i) Training their sales force to inform sample recipients in a meaningful manner that samples may not be sold or billed (thus vitiating any monetary value of the sample); (ii) clearly and conspicuously labeling individual samples as units that may not be sold (thus minimizing the ability of recipients to advertently or inadvertently commingle samples with purchased product); and (iii) including on packaging and any documentation related to the samples (such as shipping notices or invoices) a clear and conspicuous notice that the samples are subject to PDMA and may not be sold. Recent government enforcement activity has focused on instances in which drug samples were provided to physicians who, in turn, sold them to the patient or billed them to the federal health care programs on behalf of the patient.

C. Designation of a Compliance Officer and a Compliance Committee

1. Compliance Officer

Every pharmaceutical manufacturer should designate a compliance officer to serve as the focal point for compliance activities.[12] This responsibility may be the individual's sole duty or added to other management responsibilities, depending upon the size and resources of the company and the complexity of the task. If the individual has additional management responsibilities, the pharmaceutical manufacturer should ensure that the individual is able to dedicate adequate and substantive time and attention to the compliance functions. Similarly, if the compliance officer delegates some of the compliance duties, he or she should, nonetheless, remain sufficiently involved to fulfill the compliance oversight function.

Designating a compliance officer with the appropriate authority is critical to the success of the program, necessitating the appointment of a high-level official with direct access to the company's president or CEO, board of directors, all other senior management, and legal counsel. The compliance officer should have sufficient funding, resources, and staff to perform his or her responsibilities fully. The compliance officer should be able to effectuate change within the organization as necessary or appropriate and to exercise independent judgment. Optimal placement of the compliance officer within the organization will vary according to the particular situation of a manufacturer.[13]

Coordination and communication with other appropriate individuals or business units are the key functions of the compliance officer with regard to planning, implementing or enhancing, and monitoring the compliance program. The compliance officer's primary responsibilities should include:

- Overseeing and monitoring implementation of the compliance program; [14]
- Reporting on a regular basis to the company's board of directors, CEO or president, and compliance committee (if applicable) on compliance matters and assisting these individuals or groups to establish methods to reduce the company's vulnerability to fraud and abuse;
- Periodically revising the compliance program, as appropriate, to respond to changes in the company's needs and applicable federal health care program requirements, identified weakness in the compliance program, or identified systemic patterns of noncompliance;
- Developing, coordinating, and participating in a multifaceted educational and training program that focuses on the elements of the compliance program, and seeking to ensure that all affected employees and management understand and comply with pertinent federal and state standards;
- Ensuring that independent contractors and agents, particularly those agents and contractors who are involved in sales and marketing activities, are aware of the requirements of the company's compliance program with respect to sales and marketing activities, among other things;
- Coordinating personnel issues with the company's Human Resources/

Personnel office (or its equivalent) to ensure that the List of Excluded Individuals/Entities [15] has been checked with respect to all employees and independent contractors;

- Assisting the company's internal auditors in coordinating internal compliance review and monitoring activities;
- Reviewing and, where appropriate, acting in response to reports of noncompliance received through the hotline (or other established reporting mechanism) or otherwise brought to his or her attention (*e.g.*, as a result of an internal audit or by corporate counsel who may have been notified of a potential instance of noncompliance);
- Independently investigating and acting on matters related to compliance. To that end, the compliance officer should have the flexibility to design and coordinate internal investigations (*e.g.*, responding to reports of problems or suspected violations) and any resulting corrective action (*e.g.*, making necessary improvements to policies and practices, and taking appropriate disciplinary action) with various company divisions or departments;
- Participating with the company's counsel in the appropriate reporting of any self-discovered violations of federal health care program requirements; and
- Continuing the momentum and, as appropriate, revision or expansion of the compliance program after the initial years of implementation.[16]

The compliance officer must have the authority to review all documents and other information relevant to compliance activities. This review authority should enable the compliance officer to examine interactions with government programs to determine whether the company is in compliance with federal health care program reporting and rebate requirements and to examine interactions with health care professionals that could violate kickback prohibitions or other federal health care programs requirements. Where appropriate, the compliance officer should seek the advice of competent legal counsel about these matters.

2. Compliance Committee

The OIG recommends that a compliance committee be established to advise the compliance officer and assist in the implementation of the compliance program.[17] When developing an appropriate team of people to serve as the pharmaceutical manufacturer's compliance committee, the company should consider a variety of skills and personality traits that are expected from the team members. The company should expect its compliance committee members and compliance officer to demonstrate high integrity, good judgment, assertiveness, and an approachable demeanor, while eliciting the respect and trust of company employees. These interpersonal skills are as important as the professional experience of the compliance officer and each member of the compliance committee.

Once a pharmaceutical manufacturer chooses the people who will accept the responsibilities vested in members of the compliance committee, the company needs to train these individuals on the policies and procedures of the compliance program, as well as how to discharge their duties. The OIG recognizes that some pharmaceutical manufacturers (*e.g.*, small companies or those with limited budgets) may not have the resources or the need to establish a compliance committee. However, when potential problems are identified at such companies, the OIG recommends the creation of a "task force" to address the particular issues. The members of the task force may vary depending upon the area of concern. For example, if the compliance officer identifies issues relating to improper inducements to the company's purchasers or prescribers, the OIG recommends that a task force be organized to review the arrangements and interactions with those purchasers or prescribers. In essence, the compliance committee is an extension of the compliance officer and provides the organization with increased oversight.

D. Conducting Effective Training and Education

The proper education and training of officers, directors, employees, contractors, and agents, and periodic retraining of personnel at all levels are critical elements of an effective compliance program. A pharmaceutical manufacturer must take steps to communicate effectively its standards and procedures to all affected personnel by requiring participation in appropriate training programs and by other means, such as disseminating publications that explain specific requirements in a practical manner. These training programs should include general sessions summarizing the manufacturer's compliance program, written standards, and applicable federal health care program requirements. All employees and, where feasible and appropriate, contractors should receive the general training. More specific training on issues, such as (i) the anti-kickback statute and how it applies to pharmaceutical sales and marketing practices and (ii) the calculation and reporting of pricing information and payment of rebates in connection with federal health care programs, should be targeted at those employees and contractors whose job requirements make the information relevant. The specific training should be tailored to make it as meaningful as possible for each group of participants.

Managers and employees of specific divisions can assist in identifying specialized areas that require training and in carrying out such training. Additional areas for training may also be identified through internal audits and monitoring and from a review of any past compliance problems of the pharmaceutical manufacturer or similarly situated companies. A pharmaceutical manufacturer should regularly review its training and, where appropriate, update the training to reflect issues identified through audits or monitoring and any relevant changes in federal health care program requirements. Training instructors may come from outside or inside the organization, but must be qualified to present the subject matter involved and sufficiently experienced in the issues presented to adequately field questions and coordinate discussions among those being trained. Ideally, training instructors should be available for follow-up questions after the formal training session has been conducted.

The pharmaceutical manufacturer should train new employees soon after they have started working. Training programs and materials should be designed to take into account the skills, experience, and knowledge of the individual trainees. The compliance officer should document any formal training undertaken by the company as part of the compliance program. The company should retain adequate records of its training of employees, including attendance logs, descriptions of the training sessions, and copies of the material distributed at training sessions.

The OIG suggests that all relevant personnel (*i.e.*, employees as well as agents of the pharmaceutical manufacturer) participate in the various educational and training programs of the company. For example, for sales representatives who are responsible for the sale and marketing of the company's products, periodic training in the anti-kickback statute and its safe harbors should be required. Employees should be required to have a minimum number of educational hours per year, as appropriate, as part of their employment responsibilities.

The OIG recognizes that the format of the training program will vary depending upon the size and resources of the pharmaceutical manufacturer. For example, a company with limited resources or whose sales force is widely dispersed may want to create a videotape or computer-based program for each type of training session so new employees and employees outside of central locations can receive training in a timely manner. If videos or computer-based programs are used for compliance training, the OIG suggests that the company make a qualified individual available to field questions from trainees. Also, large pharmaceutical manufacturers may find training via the Internet or video conference capabilities to be a cost-effective means of reaching a large number of employees. Alternatively, large companies may include training sessions as part of regularly scheduled regional meetings.

The OIG recommends that participation in training programs be made a condition of continued employment and that failure to comply with training requirements should result in disciplinary action. Adherence to the training requirements as well as other provisions of the compliance program should be a factor in the annual evaluation of each employee.

E. Developing Effective Lines of Communication

1. Access to Supervisors and/or the Compliance Officer

In order for a compliance program to work, employees must be able to ask questions and report problems. Supervisors play a key role in responding to employee concerns and it is appropriate that they serve as a first line of communications. Pharmaceutical manufacturers should consider the adoption of open-door policies in order to foster dialogue between management and employees. In order to encourage communications, confidentiality and non-retaliation policies should also be developed and distributed to all employees.[18]

Open lines of communication between the compliance officer and employees are equally important to the successful implementation of a compliance program and the reduction of any potential for fraud and abuse. In addition to serving as a contact point for reporting problems and initiating appropriate responsive action, the compliance officer should be viewed as someone to whom personnel can go to get clarification on the company's policies. Questions and responses should be documented and dated and, if appropriate, shared with other staff so that compliance standards or polices can be updated and improved to reflect any necessary changes or clarifications. Pharmaceutical manufacturers may also consider rewarding employees for appropriate use of established reporting systems as a way to encourage the use of such systems.

2. Hotlines and Other Forms of Communication

The OIG encourages the use of hotlines, e-mails, newsletters, suggestion boxes, and other forms of information exchange to maintain open lines of communication. In addition, an effective employee exit interview program could be designed to solicit information from departing employees regarding potential misconduct and suspected violations of company policy and procedures. Pharmaceutical manufacturers may also identify areas of risk or concern through periodic surveys or communications with sales representatives about the current marketing environment. This could provide management with insight about and an opportunity to address conduct occurring in the field, either by the company's own sale representatives or those of other companies.

If a pharmaceutical manufacturer establishes a hotline or other reporting mechanism, information regarding how to access the reporting mechanism should be made readily available to all employees and independent contractors by including that information in the code of conduct or by circulating the information (*e.g.*, by publishing the hotline number or e-mail address on wallet cards) or conspicuously posting the information in common work areas. Employees should be permitted to report matters on an anonymous basis.

Reported matters that suggest substantial violations of compliance policies or applicable Federal health care program requirements should be documented and investigated promptly to determine their veracity and the scope and cause of any underlying problem. The compliance officer should maintain a detailed log that records such reports, including the nature of any investigation, its results, and any remedial or disciplinary action taken. Such information, redacted of individual identifiers, should be summarized and included in reports to the board of directors, the president or CEO, and compliance committee. Although the pharmaceutical manufacturer should always strive to maintain the confidentiality of an employee's identity, it should also make clear that there might be a point where the individual's identity may become known or need to be revealed in certain instances. The OIG recognizes that protecting anonymity may be infeasible for small companies. However, the OIG believes all employees, when seeking answers to questions or reporting potential instances of fraud and abuse, should know to whom to turn for a meaningful response and should be able to do so without fear of retribution.

F. Auditing and Monitoring

An effective compliance program should incorporate thorough monitoring of its implementation and an ongoing evaluation process. The compliance officer should document this ongoing monitoring, including reports of suspected noncompliance, and provide these assessments to company's senior management and the compliance committee. The extent and frequency of the compliance audits may vary depending on variables such as the pharmaceutical manufacturer's available resources, prior history of noncompliance, and the risk factors particular to the company. The nature of the reviews may also vary and could include a prospective systemic review of the manufacturer's processes, protocols, and practices or a retrospective review of actual practices in a particular area.

Although many assessment techniques are available, it is often effective to have internal or external evaluators who have relevant expertise perform regular compliance reviews. The reviews should focus on those divisions or departments of the pharmaceutical manufacturer that have substantive involvement with or impact on federal health care programs (such as the government contracts and sales and marketing divisions) and on the risk areas identified in this guidance. The reviews should also evaluate the company's policies and procedures regarding other areas of concern identified by the OIG (*e.g.*, through Special Fraud Alerts) and federal and state law enforcement agencies. Specifically, the reviews should evaluate whether the: (1) Pharmaceutical manufacturer has policies covering the identified risk areas; (2) policies were implemented and communicated; and (3) policies were followed.

G. Enforcing Standards Through Well-Publicized Disciplinary Guidelines

An effective compliance program should include clear and specific disciplinary policies that set out the consequences of violating the law or the pharmaceutical manufacturer's code of

conduct or policies and procedures. A pharmaceutical manufacturer should consistently undertake appropriate disciplinary action across the company in order for the disciplinary policy to have the required deterrent effect. Intentional and material noncompliance should subject transgressors to significant sanctions. Such sanctions could range from oral warnings to suspension, termination or other sanctions, as appropriate. Disciplinary action also may be appropriate where a responsible employee's failure to detect a violation is attributable to his or her negligence or reckless conduct. Each situation must be considered on a case-by-case basis, taking into account all relevant factors, to determine the appropriate response.

H. Responding to Detected Problems and Developing Corrective Action Initiatives

Violation of a pharmaceutical manufacturer's compliance program, failure to comply with applicable federal or state law, and other types of misconduct threaten the company's status as a reliable, honest, and trustworthy participant in the health care industry. Detected but uncorrected misconduct can endanger the reputation and legal status of the company. Consequently, upon receipt of reasonable indications of suspected noncompliance, it is important that the compliance officer or other management officials immediately investigate the allegations to determine whether a material violation of applicable law or the requirements of the compliance program has occurred and, if so, take decisive steps to correct the problem.[19] The exact nature and level of thoroughness of the investigation will vary according to the circumstances, but the review should be detailed enough to identify the root cause of the problem. As appropriate, the investigation may include a corrective action plan, a report and repayment to the government, and/or a referral to criminal and/or civil law enforcement authorities.

Reporting

Where the compliance officer, compliance committee, or a member of senior management discovers credible evidence of misconduct from any source and, after a reasonable inquiry, believes that the misconduct may violate criminal, civil, or administrative law, the company should promptly report the existence of misconduct to the appropriate federal and state authorities[20] within a reasonable period, but not more than 60 days,[21] after determining that there is credible evidence of a violation.[22] Prompt voluntary reporting will demonstrate the pharmaceutical manufacturer's good faith and willingness to work with governmental authorities to correct and remedy the problem. In addition, reporting such conduct will be considered a mitigating factor by the OIG in determining administrative sanctions (*e.g.*, penalties, assessments, and exclusion), if the reporting company becomes the subject of an OIG investigation.[23]

When reporting to the government, a pharmaceutical manufacturer should provide all information relevant to the alleged violation of applicable federal or state law(s) and the potential financial or other impact of the alleged violation. The compliance officer, under advice of counsel and with guidance from the governmental authorities, could be requested to continue to investigate the reported violation. Once the investigation is completed, and especially if the investigation ultimately reveals that criminal, civil or administrative violations have occurred, the compliance officer should notify the appropriate governmental authority of the outcome of the investigation, including a description of the impact of the alleged violation on the operation of the applicable federal health care programs or their beneficiaries.

III. Conclusion

In today's environment of increased scrutiny of corporate conduct and increasingly large expenditures for prescription drugs, it is imperative for pharmaceutical manufacturers to establish and maintain effective compliance programs. These programs should foster a culture of compliance that begins at the executive level and permeates throughout the organization. This compliance guidance is designed to provide assistance to all pharmaceutical manufacturers as they either implement compliance programs or re-assess existing programs. The essential elements outlined in this compliance guidance can be adapted to the unique environment of each manufacturer. It is the hope and expectation of the OIG that the resulting compliance programs will benefit not only federal health care programs and their beneficiaries, but also pharmaceutical manufacturers themselves.

Dated: April 23, 2003.

Janet Rehnquist,

Inspector General.

Endnotes

1. The term "Federal health care programs," as defined in 42 U.S.C. 1320a–7b(f), includes 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 or any state health plan (*e.g.*, Medicaid or a program receiving funds from block grants for social services or child health services). In this document, the term "federal health care program requirements" refers to the statutes, regulations and other rules governing Medicare, Medicaid, and all other federal health care programs.

2. *See* 66 FR 31246 (June 11, 2001), "Notice for Solicitation of Information and Recommendations for Developing a Compliance Program Guidance for the Pharmaceutical Industry."

3. *See* 67 FR 62057 (October 3, 2002), "Draft OIG Compliance Program Guidance for Pharmaceutical Manufacturers."

4. 42 U.S.C. 1320a–7b(b).

5. In addition, the compliance program elements and potential risk areas addressed in this compliance program guidance may also have application to manufacturers of other products that may be reimbursed by federal health care programs, such as medical devices and infant nutritional products.

6. In addition, pharmaceutical manufacturers should be mindful that many states have fraud and abuse statutes—including false claims, anti-kickback and other statutes—that are not addressed in this guidance.

7. The False Claims Act (31 U.S.C. 3729–33) prohibits knowingly presenting (or causing to be presented) to the federal government a false or fraudulent claim for payment or approval. Additionally, it prohibits knowingly making or using (or causing to be made or used) a false record or statement to get a false or fraudulent claim paid or approved by the federal government or its agents, like a carrier, other claims processor, or state Medicaid program.

8. The 340B Program, contained as part of the Public Health Services Act and codified at 42 U.S.C. 256b, is administered by the Health Resources and Services Administration (HRSA).

9. 42 U.S.C. 1396r–8. Average Manufacturer Price and Best Price are defined in the statute at 42 U.S.C. 1396r–8(k)(1) and 1396r–8(c)(1), respectively. CMS has provided further guidance on these terms in the National Drug Rebate Agreement and in Medicaid Program Releases available through its Web site at *http://www.hcfa.gov/medicaid/drugs/drug.mpg.htm.*

10. In this regard, pharmaceutical manufacturers should note that the exception for non-monetary compensation under the Stark law (42 U.S.C. 1395nn; 42 CFR 411.357(k)) is not a basis for protection under the anti-kickback statute.

11. CME programs with no industry sponsorship, financing, or affiliation should not raise anti-kickback concerns, although tuition payments by manufacturers (or their representatives) for persons in a position to influence referrals (*e.g.*, physicians or medical students) may raise concerns.

12. It is also advisable to designate as a compliance officer an individual with prior experience or knowledge of compliance and

operational issues relevant to pharmaceutical manufacturers.

13. The OIG believes it is generally not advisable for the compliance function to be subordinate to the pharmaceutical manufacturer's general counsel, or comptroller or similar financial officer. Separation of the compliance function helps to ensure independent and objective legal reviews and financial analysis of the company's compliance efforts and activities. By separating the compliance function from the key management positions of general counsel or chief financial officer (where the size and structure of the pharmaceutical manufacturer make this a feasible option), a system of checks and balances is established to more effectively achieve the goals of the compliance program.

14. For companies with multiple divisions or regional offices, the OIG encourages coordination with each company location through the use of a compliance officer located in corporate headquarters who is able to communicate with parallel compliance liaisons in each division or regional office, as appropriate.

15. As part of its commitment to compliance, a pharmaceutical manufacturer should carefully consider whether to hire or do business with individuals or entities that have been sanctioned by the OIG. The List of Excluded Individuals and Entities can be checked electronically and is accessible through the OIG's Web site at: *http://oig.hhs.gov*.

16. There are many approaches the compliance officer may enlist to maintain the vitality of the compliance program. Periodic on-site visits of regional operations, bulletins with compliance updates and reminders, distribution of audiotapes, videotapes, CD ROMs, or computer notifications about different risk areas, lectures at management and employee meetings, and circulation of recent articles or publications discussing fraud and abuse are some examples of approaches the compliance officer may employ.

17. The compliance committee benefits from having the perspectives of individuals with varying responsibilities and areas of knowledge in the organization, such as operations, finance, audit, human resources, legal, and sales and marketing, as well as employees and managers of key operating units. The compliance officer should be an integral member of the committee. All committee members should have the requisite seniority and comprehensive experience within their respective departments to recommend and implement any necessary changes to policies and procedures.

18. In some cases, employees sue their employers under the False Claims Act's *qui tam* provisions after a failure or apparent failure by the company to take action when the employee brought a questionable, fraudulent, or abusive situation to the attention of senior corporate officials. Whistleblowers must be protected against retaliation, a concept embodied in the provisions of the False Claims Act. *See* 31 U.S.C. 3730(h).

19. Instances of noncompliance must be determined on a case-by-case basis. The existence or amount of a *monetary* loss to a federal health care program is not solely determinative of whether the conduct should be investigated and reported to governmental authorities. In fact, there may be instances where there is no readily identifiable monetary loss, but corrective actions are still necessary to protect the integrity of the health care program.

20. Appropriate federal and state authorities include the OIG, the Criminal and Civil Divisions of the Department of Justice, the U.S. Attorney in relevant districts, the Food and Drug Administration, the Federal Trade Commission, the Drug Enforcement Administration and the Federal Bureau of Investigation, and the other investigative arms for the agencies administering the affected federal or state health care programs, such as the state Medicaid Fraud Control Unit, the Defense Criminal Investigative Service, the Department of Veterans Affairs, HRSA, and the Office of Personnel Management (which administers the Federal Employee Health Benefits Program).

21. In contrast, to qualify for the "not less than double damages" provision of the False Claims Act, the provider must provide the report to the government within 30 days after the date when the provider first obtained the information. 31 U.S.C. 3729(a).

22. Some violations may be so serious that they warrant immediate notification to governmental authorities prior to, or simultaneous with, commencing an internal investigation. By way of example, the OIG believes a provider should report misconduct that: (1) Is a clear violation of administrative, civil, or criminal laws; (2) has a significant adverse effect on the quality of care provided to federal health care program beneficiaries; or (3) indicates evidence of a systemic failure to comply with applicable laws or an existing corporate integrity agreement, regardless of the financial impact on federal health care programs.

23. The OIG has published criteria setting forth those factors that the OIG takes into consideration in determining whether it is appropriate to exclude an individual or entity from program participation pursuant to 42 U.S.C. 1320a–7(b)(7) for violations of various fraud and abuse laws. *See* 62 FR 67392 (December 24, 1997).

[FR Doc. 03–10949 Filed 5–2–03; 8:45 am]
BILLING CODE 4152–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Substance Abuse and Mental Health Services Administration

Agency Information Collection Activities: Submission for OMB Review; Comment Request

Periodically, the Substance Abuse and Mental Health Services Administration (SAMHSA) will publish a summary of information collection requests under OMB review, in compliance with the Paperwork Reduction Act (44 U.S.C. Chapter 35). To request a copy of these documents, call the SAMHSA Reports Clearance Officer on (301) 443–7978.

National Evaluation of the Comprehensive Community Mental Health Services for Children and Their Families Program: Phase Three—(OMB No. 0930–0209, revision)—SAMHSA's Center for Mental Health Services is conducting Phase III of the national evaluation of the Comprehensive Community Mental Health Services for Children and Their Families Program. Phase III collects data on child mental health outcomes, family life, and service system development and performance. Data are being collected on 22 funded systems of care, and approximately 5,100 children and families. Data collection for this evaluation will be conducted over a 5½-year period.

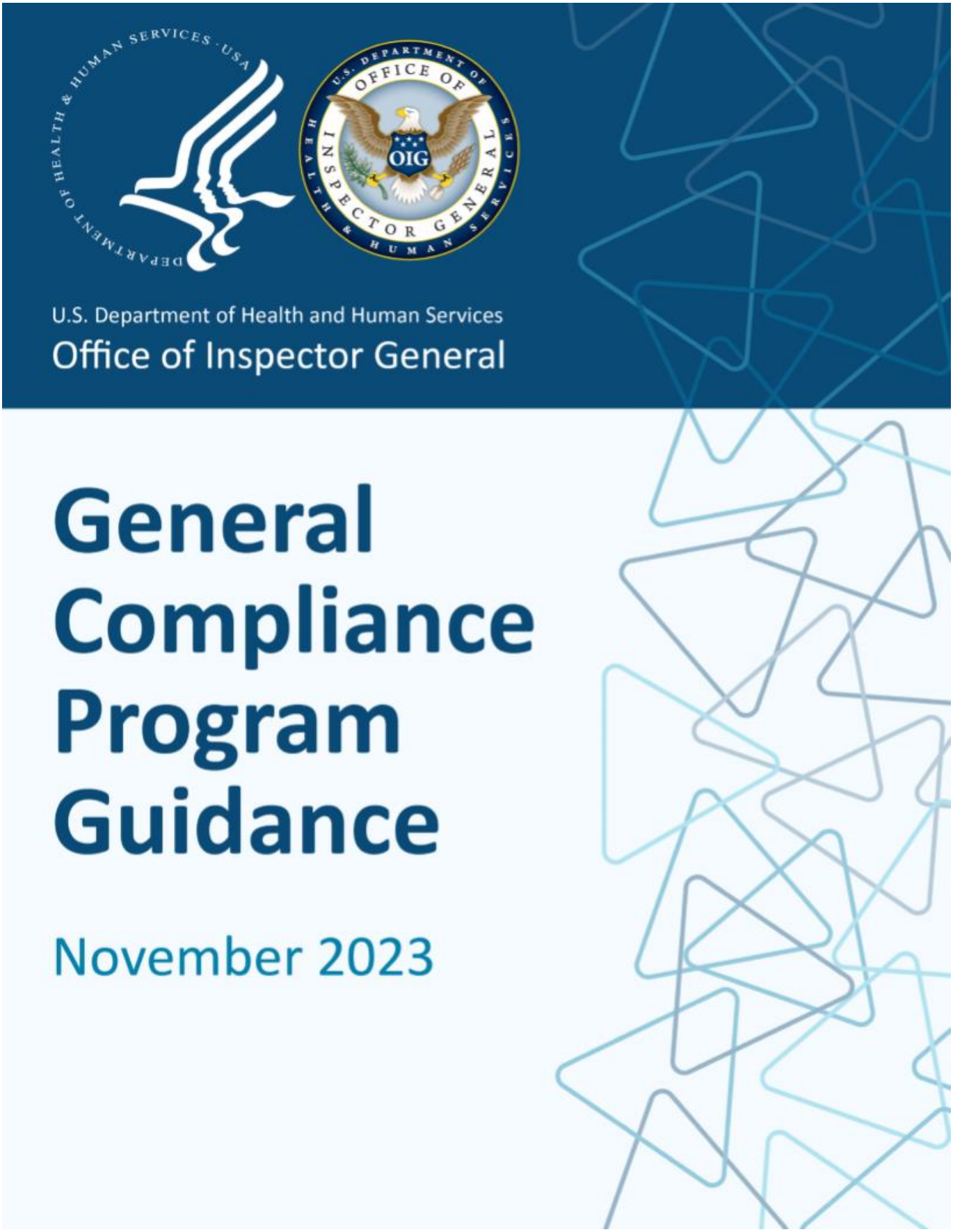
The core of service system data are currently collected every 18 months throughout the evaluation period. Service delivery and system variables of interest include the following: Maturity of system of care development, adherence to the system of care program model, and client service experience. The length of time that individual families will participate in the study ranges from 18 to 36 months depending on when they enter the evaluation.

Child and family outcomes of interest will be collected at intake and during subsequent follow-up sessions at six-month intervals. The outcome measures include the following: Child symptomatology and functioning, family functioning, material resources, and caregiver strain. In addition, a treatment effectiveness study will examine the relative impact of an evidence-based treatment within one system of care.

The average annual respondent burden is estimated below. The estimate reflects the average number of respondents in each respondent category, the average number of responses per respondent per year, the average length of time it will take for each response, and the total average annual burden for each category of respondent, and for all categories of respondents combined.

This revision to the currently approved information collection activities involves: (1) Extension of the data collection period for an additional 18 months to cover an additional sixth year of grant funding in the 22 currently funded systems of care (and a six-month no-cost extension for the evaluation), (2) the addition of a family-driven study to assess the extent of family involvement in service planning, (3) the elimination of the longitudinal comparison study and the addition of a treatment effectiveness study in two sites

HHS OIG's 2023 General Compliance Program Guidance



User's Guide

Welcome to OIG's General Compliance Program Guidance (GCPG).

The GCPG is a reference guide for the health care compliance community and other health care stakeholders. The GCPG provides information about relevant Federal laws, compliance program infrastructure, OIG resources, and other information useful to understanding health care compliance.

The GCPG is voluntary guidance that discusses general compliance risks and compliance programs. The GCPG is not binding on any individual or entity. Of note, OIG uses the word "should" in the GCPG to present voluntary, nonbinding guidance.

The GCPG's detailed table of contents allows the user to directly access the specific topic they are interested in, such as the Federal anti-kickback statute, the compliance officer role, or quality considerations. Many sections contain links to other parts of the GCPG, OIG's website, or other Internet locations that contain useful information, including related topics within the GCPG, OIG compliance resources, the current text of laws and regulations, and other information OIG believes users may find valuable.

The GCPG may be accessed on the Internet, downloaded to the user's computer, or printed and distributed in hard copy. Using the GCPG on a computer will allow the user to efficiently navigate the GCPG and access the links OIG has embedded throughout the document.

The GCPG contains some unique defined terms. These terms are hyperlinked to their definition. Users who choose to print a hard copy of one or more sections of the GCPG, but not the GCPG in its entirety, should be mindful that the definitions may not be contained in the printed sections. Users should consider copying definitions of any terms defined outside of their individualized sections and including those definitions with the hard-copy document.

Users who read the GCPG from beginning to end may find that it repeats certain information. This is because OIG recognizes that users may read, or may later reference, specific sections only, and not the whole document. Therefore, relevant information may be included and repeated in multiple sections.

HHS Office of Inspector General

Table of Contents

HHS Office of Inspector General

HHS Office of Inspector General

HHS Office of Inspector General

6

I. Introduction

Since its establishment in 1976 and consistent with its statutory charge, the Department of Health and Human Services (HHS) Office of Inspector General (OIG) has been at the forefront of the Nation's efforts to fight fraud, waste, and abuse and improve the efficiency of Medicare, Medicaid, and more than 100 other HHS programs. OIG is the largest civilian inspector general's office in the Federal Government.

A. OIG's History of Compliance Program Guidance: Commitment to Preventing Health Care Fraud and Abuse

OIG developed compliance program guidance documents (CPGs) as voluntary, nonbinding guidance documents to support health care industry stakeholders in their efforts to self-monitor compliance with applicable laws and program requirements. These include CPGs directed at: (1) hospitals; (2) home health agencies; (3) clinical laboratories; (4) third-party medical billing companies; (5) the durable medical equipment, prosthetics, orthotics, and supply industry; (6) hospices; (7) Medicare Advantage (formerly known as Medicare+Choice) organizations; (8) nursing facilities; (9) physicians; (10) ambulance suppliers; and (11) pharmaceutical manufacturers.

B. OIG's Current Compliance Guidance Approach: A Roadmap Going Forward

Based on feedback received as part of OIG's Modernization Initiative and other input, we understand that CPGs have served as an important and valuable OIG resource for the health care compliance community and industry stakeholders since publication of the first CPG in 1998. OIG has carefully considered ways to improve and update existing CPGs and to deliver new CPGs specific to segments of the health care industry and to entities involved in the health care industry that have emerged in the past two decades. In modernizing OIG's CPGs, our goal is to produce useful, informative resources to help advance the industry's voluntary compliance efforts in preventing fraud, waste, and abuse in the health care system.

In an effort to produce user-friendly and accessible information and to promote greater flexibility to update CPGs as new risk areas emerge, OIG will no longer publish updated or new

Return to TOC

HHS Office of Inspector General

7

CPGs in the OIG will no longer publish updated or new CPGs in the *Federal Register*. All current, updated, and new CPGs will be available on our website with interactive links to resources. OIG is using the following format to make our guidance more user-friendly and accessible:

First, our General CPG (GCPG) applies to all individuals and entities involved in the health care industry. The GCPG addresses: key Federal authorities for entities engaged in health care business; the seven elements of a compliance program; adaptations for small and large entities; other compliance considerations; and OIG processes and resources. We anticipate updating the GCPG as changes in compliance practices or legal requirements may warrant.

Second, starting in 2024, we will be publishing industry segment-specific CPGs (ICPGs) for different types of providers, suppliers, and other participants in health care industry subsectors or ancillary industry sectors relating to Federal health care programs. ICPGs will be tailored to fraud and abuse risk areas for each industry subsector and will address compliance measures that the industry subsector participants can take to reduce these risks. ICPGs are intended to be updated periodically to address newly identified risk areas and compliance measures and to ensure timely and meaningful guidance from OIG.

GCPG

- Key Federal authorities for entities engaged in health care business
- Seven elements of a compliance program
- Adaptations for small and large entities
- Other compliance considerations
- OIG process and resources

ICPGs

- For different types of providers, suppliers, and other participants in health care industry subsectors or ancillary industry sectors
- Tailored to fraud and abuse risk areas for each industry subsector
- Compliance measures that participants can take to reduce risk.

OIG welcomes feedback from the health care community and other stakeholders in connection with the GCPG and forthcoming ICPGs. We have designated an email inbox at Compliance@oig.hhs.gov where any such feedback can be submitted.

Return to TOC

Tip **It is important to note that OIG has several options for receiving communications about questions unrelated to the GCPG or ICPGs. For example, questions regarding exclusions can be directed to exclusions@oig.hhs.gov, and questions of a general nature can be directed to Public.Affairs@oig.hhs.gov. For a full list of how best to contact OIG, see the agency's Contact Us website.**

For the GCPG, the type of feedback sought includes general compliance considerations and suggestions for general risk areas to include in the GCPG or other resources. For the ICPGs, we are seeking suggestions for risk areas specifically related to the different types of providers, suppliers, and other participants in health care industry subsectors or ancillary industry sectors that are addressed in a particular ICPG. Submissions will generate an automated confirmation of receipt, which will be the only response to a submission unless additional follow-up is needed. In that instance, OIG may reach out directly to the sender for the relevant submission.

C. Application of the GCPG and ICPGs

OIG's existing CPGs, this GCPG, and our forthcoming ICPGs do not constitute a model compliance program. The GCPG and ICPGs are for use as a resource by the health care community; they are not intended to be one-size-fits-all, completely comprehensive, or all-inclusive of compliance considerations and fraud and abuse risks for every organization. Rather, the goal of these documents has been, and will continue to be, to set forth voluntary compliance guidelines and tips and to identify some risk areas that OIG believes individuals and entities engaged in the health care industry should consider when developing and implementing a new compliance program or evaluating and updating an existing one. Our existing CPGs and supplemental CPGs will remain available for use as an ongoing resource to help identify risk areas in particular industry subsectors as we develop the ICPGs. Existing CPGs will be archived but still available on our website when ICPGs are issued.

Return to TOC

SECTION II
Health Care Fraud Enforcement and Other Standards: Overview of Certain Federal Laws

II. Health Care Fraud Enforcement and Other Standards: Overview of Certain Federal Laws

This guidance does not create any new law or legal obligations, and the discussions in this guidance are not intended to present detailed or comprehensive summaries of lawful or unlawful activity.

Critical to understanding compliance risks and the framework overlaying compliance programs is a working knowledge of applicable law. Consequently, the GCPG begins with an overview of certain Federal authorities that may apply to entities involved in health care, which include the primary Federal fraud and abuse laws and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules. These overviews are intended to be summaries only and they do not address every legal obligation that may be imposed on the health care community and affiliated partners. For example, we note that this guidance—and these legal overviews—do not address State fraud and abuse laws. In addition, these overviews do not establish or interpret any program rules or regulations. Our goal in summarizing certain key Federal authorities is to create awareness and provide tools and resources to aid compliance efforts in both preventing violations and identifying potential red flags early with respect to these laws and regulations. Government agencies, including the Department of Justice (DOJ), OIG, the Centers for Medicare & Medicaid Services (CMS), and the HHS Office for Civil Rights (OCR), are charged with interpreting and enforcing these laws and regulations. It is crucial to understand these authorities not only because following them is the right thing to do, but also because violating them could result in an obligation to repay overpayments, criminal penalties, civil or administrative fines, and exclusion from the Federal health care programs.

A. Federal Anti-Kickback Statute

The Federal anti-kickback statute prohibits entities involved in Federal health care program business from engaging in some practices that are common in other business sectors, such as offering or receiving gifts to reward past or future referrals. As a general matter, the Federal anti-kickback statute is an intent-based, criminal statute that prohibits remuneration, whether monetary, in-kind, or in other forms, in exchange for referrals of Federal health care program business. More specifically, under the Federal anti-kickback statute, it is a criminal offense to

Return to TOC

HHS Office of Inspector General

knowingly and willfully offer, pay, solicit, or receive any remuneration to induce, or in return for, the referral of an individual to a person for the furnishing of, or arranging for the furnishing of, any item or service reimbursable under a Federal health care program.[1] The statute's prohibition also extends to remuneration to induce, or in return for, the purchasing, leasing, or ordering of, or arranging for or recommending the purchasing, leasing, or ordering of, any good, facility, service, or item reimbursable by a Federal health care program.[2] The statute covers activity occurring directly or indirectly as well as overtly or covertly in all instances.

For purposes of the Federal anti-kickback statute, "remuneration" includes anything of value, whether in cash, in kind, or other form. By way of example only, remuneration may take the form of cash, cash equivalents, cost-sharing waivers or subsidies, an opportunity to earn a fee, items, space, equipment, and services—regardless of the amount of remuneration—and in some circumstances, where the remuneration has been determined to be fair market value in an arm's-length transaction. The statute has been interpreted to cover any arrangement where one purpose of the remuneration is to induce referrals for items or services reimbursable by a Federal health care program.[3]

Violation of the Federal anti-kickback statute constitutes a felony punishable by a maximum fine of $100,000, imprisonment up to 10 years, or both. Conviction also will lead to mandatory exclusion from Federal health care programs, including Medicare and Medicaid. Liability under the Federal anti-kickback statute is determined separately for each party involved. In addition, a person who commits an act described in section 1128B(b) of the Social Security Act (the "Act") may be subject to False Claims Act liability[4] and civil monetary penalties (CMPs).[5] OIG also may initiate administrative proceedings to exclude such person from Federal health care programs.[6]

Congress has developed several statutory exceptions to the Federal anti-kickback statute.[7] OIG has promulgated safe harbor regulations that specify certain practices that are not treated as an offense under the Federal anti-kickback statute and do not serve as the basis for an

---

[1] Section 1128B(b) of the Social Security Act (the "Act"), 42 U.S.C. § 1320a-7b(b).
[2] Section 1128B(b) of the Act, 42 U.S.C. § 1320a-7b(b).
[3] *E.g.*, *United States v. Nagelvoort*, 856 F.3d 1117 (7th Cir. 2017); *United States v. McClatchey*, 217 F.3d 823 (10th Cir. 2000); *United States v. Davis*, 132 F.3d 1092 (5th Cir. 1998); *United States v. Kats*, 871 F.2d 105 (9th Cir. 1989); *United States v. Greber*, 760 F.2d 68 (3d Cir. 1985).
[4] 31 U.S.C. §§ 3729–3733.
[5] Section 1128A(a)(7) of the Act, 42 U.S.C. § 1320a-7a(a)(7).
[6] Section 1128(b)(7) of the Act, 42 U.S.C. §§ 1320a-7(b)(7).
[7] Section 1128B(b)(3) of the Act, 42 U.S.C. § 1320a-7b(b)(3).

Return to TOC

exclusion.[8] In short, the safe harbors protect remuneration from resulting in liability under the statute. Compliance with a safe harbor is voluntary. Safe harbor protection is afforded only to those arrangements that squarely meet all conditions set forth in the safe harbor; the protection no longer applies if even one condition is not met. That said, failure to meet a safe harbor does not render an arrangement automatically illegal. Individuals and entities should evaluate arrangements that implicate the statute and do not fit into a safe harbor by reviewing the totality of the facts and circumstances, including the intent of the parties.

Individuals and entities should evaluate arrangements that implicate the statute and do not fit into a safe harbor by reviewing the totality of the facts and circumstances, including the intent of the parties.

When attempting to identify problematic arrangements under the Federal anti-kickback statute, some relevant inquiries to explore and consider can include the following. This list of questions is illustrative, not exhaustive, and the answers to these questions alone are not determinative as to whether an arrangement violates the Federal anti-kickback statute.

Key Questions

Nature of the relationship between the parties.

- What degree of influence do the parties have, directly or indirectly, on the generation of Federal health care program business for each other?

Manner in which participants were selected.

- Were parties selected to participate in an arrangement in whole or in part because of their past or anticipated referrals?

Manner in which the remuneration is determined.

- Does the remuneration take into account, either directly or indirectly, the volume or value of business generated?

[8] 42 C.F.R. § 1001.952. OIG most recently published a final rule, Revisions to Safe Harbors Under the Anti-Kickback Statute, and Civil Monetary Penalty Rules Regarding Beneficiary Inducements, 85 Fed. Reg 77684 (Dec. 2, 2020) (the "OIG Final Rule"), which implemented seven new safe harbors, modified four existing safe harbors, and codified one new exception under the CMP provision prohibiting inducements to beneficiaries.

Return to TOC

13

- Is the remuneration conditioned in whole or in part on referrals or other business generated between the parties?
  Is the arrangement itself conditioned, either directly or indirectly, on the volume or value of Federal health care program business? Is there any service provided other than referrals?

Value of the remuneration.

- Is the remuneration fair market value in an arm's-length transaction for legitimate, reasonable, and necessary services that are actually rendered?
- Is the entity paying an inflated rate to a potential referral source?
  Is the entity receiving free or below-market-rate items or services from a provider, supplier, or other entity involved in health care business?
- Is compensation tied, either directly or indirectly, to Federal health care program reimbursement?
- Is the determination of fair market value based upon a reasonable methodology that is uniformly applied and properly documented?

Nature of items or services provided.

- Are the items and services actually needed and rendered, commercially reasonable, and necessary to achieve a legitimate business purpose?

Federal program impact.

- Does the remuneration have the potential to affect costs to any of the Federal health care programs or their beneficiaries?
- Could the remuneration lead to overutilization or inappropriate utilization?

Clinical decision making.

- Does the arrangement or practice have the potential to interfere with, or skew, clinical decision making?
- Does the arrangement or practice raise patient safety or quality of care concerns?
- Could the payment structure lead to cherry-picking healthy patients or lemon-dropping patients with chronic or other potentially costly conditions to save on costs?

Steering.

- Does the arrangement or practice raise concerns related to steering patients or health care entities to a particular item or service, or steering to a particular health care entity to provide, supply, or furnish items or services?

Potential conflicts of interest.

- Would acceptance of the remuneration diminish, or appear to diminish, the objectivity of professional judgment?

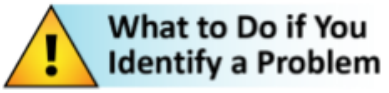
Return to TOC

HHS Office of Inspector General

- If the remuneration relates to the dissemination of information, is the information complete, accurate, and not misleading?

Manner in which the arrangement is documented.

- Is the arrangement properly and fully documented in writing?
- Are the parties documenting the items and services they provide? Are the entities monitoring items and services provided?
- Are arrangements actually conducted according to the terms of the written agreements (when written to comply with the law)?



Individuals or entities that have identified potentially problematic arrangements or practices, through these inquiries or other inquiries, can take several steps to reduce or eliminate the risk of a Federal anti-kickback statute violation, including evaluating whether an arrangement can be structured or restructured to fit within a safe harbor. If a party determines, through self-discovered evidence, that it has engaged in problematic conduct under the Federal anti-kickback statute and would like to resolve potential CMP liability with OIG, the Health Care Fraud Self-Disclosure Protocol is available to health care providers, suppliers, or other individuals or entities subject to CMPs to voluntarily self-disclose the evidence of potential fraud. More detailed information about the OIG Health Care Fraud Self-Disclosure Protocol is available here.

Return to TOC

15

B. Physician Self-Referral Law

The Federal physician self-referral (PSL) law, also known as the "Stark law," prohibits a physician from making referrals for certain designated health services (DHS) payable by Medicare[9] to an entity with which the physician (or an immediate family member) has a financial relationship, unless an exception applies and its requirements are satisfied.[10] Financial relationships include ownership and investment interests as well as compensation arrangements. For example, if a physician invests in an imaging center to which the physician refers Medicare beneficiaries for DHS, the PSL requires that the financial relationship satisfies all requirements of an applicable exception. If it does not, the PSL prohibits the physician from making a referral for DHS to be furnished by the imaging center and prohibits the imaging center from billing Medicare (or any individual, third-party payor, or other entity) for the improperly referred DHS.

Designated health services are:

- clinical laboratory services;
- physical therapy, occupational therapy, and outpatient speech-language pathology services;
- radiology and certain other imaging services;
- radiation therapy services and supplies;
- durable medical equipment and supplies;
- parenteral and enteral nutrients, equipment, and supplies;
- prosthetics, orthotics, and prosthetic devices and supplies;
- home health services;
- outpatient prescription drugs; and
- inpatient and outpatient hospital services.

Because CMS's regulations define certain categories of DHS by Current Procedural Terminology (CPT) and Healthcare Common Procedure Coding System (HCPCS) codes, CMS publishes an updated list of codes for the relevant DHS annually.

[9] In 1993, section 13624 of the Omnibus Budget Reconciliation Act (P.L. No. 103-66), "Application of Medicare Rules Limiting Certain Physician Referrals," added a new paragraph (s) to section 1903 of the Act, to extend aspects of the physician self-referral prohibitions to Medicaid. This section in part states that "no payment shall be made to a State under this section for expenditures for medical assistance under the State plan consisting of a designated health service (as defined in subsection (h)(6) of section 1877) furnished to an individual on the basis of a referral that would result in the denial of payment."

[10] Section 1877 of the Act, 42 U.S.C. § 1395nn; 42 C.F.R. §§ 411.350–11.389.

Return to TOC

HHS Office of Inspector General

16

When analyzing an arrangement under the PSL, it is important to determine whether certain key elements are present. The PSL is implicated only when **all six** of the following elements are present:[11]

1. A physician
2. Makes a referral
3. For designated health services
4. Payable by Medicare
5. To an entity
6. With which the physician (or an immediate family member) or the physician organization in whose shoes the physician stands has a financial relationship (which could be a direct or indirect ownership or investment interest in the entity or a compensation arrangement with the entity).

Where all six elements exist, the PSL prohibits a physician from making a referral for DHS to the entity with which they have the financial relationship unless an exception applies and its requirements are satisfied.

The PSL is a strict-liability statute, which means proof of intent to violate the law is not required. Penalties for physicians and entities that violate the PSL include fines as well as exclusion from participation in the Federal health care programs.[12]

Here are some examples of referrals that are likely to be prohibited under the PSL:

- Dr. X works in a physician practice located in a major city. Dr. X's sister owns a free-standing laboratory located in the same city. Dr. X refers all orders for clinical laboratory tests on Medicare patients to the sister's free-standing laboratory.
- Dr. Y agreed to serve as the medical director of a home health agency (HHA) and was paid a sum substantially above the fair market value for their services. Dr. Y routinely referred Medicare patients to the HHA for home health services.
- After 10 years of having Dr. Z on its medical staff, a hospital began paying Dr. Z a monthly stipend of $500 to assist in meeting practice expenses. Dr. Z performs no specific service for the stipend and has no obligation to repay the hospital. Dr. Z refers Medicare patients to the hospital for inpatient surgery.

[11] Definitions and exceptions to the PSL are found at Section 1877 of the Act, 42 U.S.C. § 1395nn and at 42 C.F.R. §§ 411.350–411.389.

[12] Violations of the PSL subject the billing entity to denial of payment for the DHS, refund of amounts collected from improperly submitted claims, and a CMP of up to $15,000 for each improper claim submitted. Physicians who violate the PSL may also be subject to additional fines per prohibited referral. Also, providers that enter into an arrangement that they know or should know circumvents the law may be subject to a CMP of up to $100,000 per arrangement. Section 1877(g) of the Act, 42 U.S.C. § 1395nn.

Return to TOC

HHS Office of Inspector General

What to Do if You Identify a Problem

From a compliance perspective, it is important for entities that furnish DHS to have a method to keep track of, and review closely, their financial relationships with physicians who refer Medicare patients to them. CMS, which is the Government agency charged with interpreting the PSL, has a CMS Voluntary Self-Referral Disclosure Protocol (SRDP) that enables providers of services and suppliers to self-disclose actual or potential violations of the PSL.[13] Visit CMS SRDP FAQs for additional guidance and information about the SRDP.

Through the SRDP, CMS has the authority to reduce the amount due and owing for PSL violations. For additional information regarding the PSL, including FAQs, visit CMS's Physician Self-Referral website.

Tip

It is important to understand that the PSL and the Federal anti-kickback statute are two different laws requiring separate evaluations. Once an arrangement that may implicate the PSL, the Federal anti-kickback statute, or both is identified, it is usually best to start with an assessment under the PSL because it is a strict liability statute. If the arrangement is permissible under the PSL, it still needs to be analyzed for compliance with the Federal anti-kickback statute.

C. False Claims Act

The civil False Claims Act provides a way for the Government to recover money when an individual or entity knowingly submits or causes to be submitted false or fraudulent claims for payment to the Government. The False Claims Act,[14] among other things, prohibits:

- knowingly presenting or causing to be presented to the Federal Government a false or fraudulent claim for payment or approval;
- knowingly making or using or causing to be made or used a false record or statement to have a false or fraudulent claim paid or approved by the Government; and

[13] PSL violations may give rise to FCA violations, as described in II. C. False Claims Act.
[14] 31 U.S.C. §§ 3729–3733.

Return to TOC

- knowingly making or using or causing to be made or used a false record or statement to conceal, avoid, or decrease an obligation to pay or transmit money or property to the Government.

The False Claims Act defines "knowing" and "knowingly" to mean that "a person, with respect to information—(i) has actual knowledge of the information; (ii) acts in deliberate ignorance of the truth or falsity of the information; or (iii) acts in reckless disregard of the truth or falsity of the information; and . . . no proof of specific intent to defraud is required."[15] In short, the False Claims Act defines "knowing" and "knowingly" to include not only actual knowledge but also instances in which the person acted in deliberate ignorance or reckless disregard of the truth or falsity of the information. This means individuals and entities cannot avoid liability by deliberately ignoring inaccuracies in their claims.

Filing false claims may result in liability of up to three times the programs' loss plus an additional penalty per claim filed.[16] Under the False Claims Act, each instance of an item or a service billed to Medicare or Medicaid counts as a claim, so liability can add up quickly. A few examples of health care claims that may be false include claims where the service is not actually rendered to the patient, is already provided under another claim, is upcoded, or is not supported by the patient's medical record. A claim that is tainted by illegal remuneration under the Federal anti-kickback statute or submitted in violation of the PSL is also false or fraudulent, creating liability under the civil False Claims Act.

Further, the False Claims Act contains a whistleblower provision that allows a private individual to file a lawsuit on behalf of the United States and, if appropriate, entitles that whistleblower to a percentage of any recoveries. Anyone with knowledge of potential fraud can be a whistleblower, including current or ex-business partners, hospital or office staff, patients, or competitors. There is also a criminal False Claims Act;[17] criminal penalties for submitting false claims include imprisonment and criminal fines.

[15] 31 U.S.C. § 3729(b).
[16] Per claim penalty amounts are updated periodically and published in the Federal Register (e.g., 88 Fed. Reg. 5776 (Jan. 30, 2023)).
[17] 18 U.S.C. § 287.

Return to TOC

Health care providers and other industry stakeholders should take proactive measures to ensure compliance with program rules, including regular reviews to keep billing and coding practices up-to-date as well as regular internal billing and coding audits. Even if an entity makes an innocent billing mistake, that entity still has an obligation to repay the money to the Government. The Affordable Care Act included a requirement that entities must report and repay overpayments to Medicare and Medicaid by the later of: "(A) the date which is 60 days after the date on which the overpayment was identified; or (B) the date any corresponding cost report is due, if applicable."[18] If an entity identifies billing mistakes or other non-compliance with program rules leading to an overpayment, the entity must repay the overpayments to Medicare and Medicaid to avoid False Claims Act liability.

If an entity identifies billing mistakes or other non-compliance with program rules leading to an overpayment, the entity must repay the overpayments to Medicare and Medicaid to avoid False Claims Act liability.

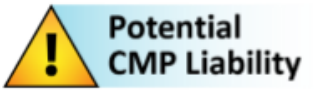
D. Civil Monetary Penalty Authorities

OIG is authorized to pursue monetary penalties and exclusion through a variety of civil authorities—most notably, the Civil Monetary Penalties Law (CMPL). Under the CMPL, OIG can pursue assessments in lieu of damages, CMPs, and exclusion from participation in the Federal health care programs. With this authority, OIG can address a wide variety of improper conduct related to Federal health care programs and other HHS programs.[19] The CMPL principally addresses fraudulent and abusive conduct. In addition to OIG's CMP authorities that closely parallel the False Claims Act, OIG has additional CMP authorities aimed at certain specific types of conduct unique to HHS and the Federal health care programs—for example, the "patient dumping" CMP.[20] **While False Claims Act cases are pursued by DOJ on behalf of HHS in Federal court, CMP cases are administrative and pursued by OIG before an HHS administrative law judge.** By statute, different categories of conduct result in different penalty amounts (for example, false claims result in penalties of up to $20,000 per item or service

[18] Section 1128J of the Act, 42 U.S.C. § 1320a-7k(d); *see also*, 42 C.F.R. §§ 401.301–305.
[19] *See* OIG Civil Monetary Penalty Authorities.
[20] Emergency Medical Treatment & Labor Act (EMTALA), Section 1867(d)(1) of the Act, 42 U.S.C. § 1395dd(d)(1).

Return to TOC

falsely claimed, and improper kickback conduct results in penalties of up to $100,000 per violation).[21]



We provide more detailed descriptions of certain CMP authorities in this section, but some illustrative examples of conduct that could lead to potential CMP liability include:

- presenting a claim that the person knows or should know is for an item or service that was not provided as claimed or is false or fraudulent;[22]
- arranging for or contracting (by employment or otherwise) with an individual or entity that the person knows or should know is excluded from participation in a Federal health care program for the purpose of providing items and services for which payment may be made by a Federal health care program;[23]
- presenting a claim for a pattern of medical or other items or services that a person knows or should know are not medically necessary;[24]
- committing acts described in the Federal anti-kickback statute;[25]
- failing to report and return a known overpayment;[26]
- failing to provide an adequate medical screening examination for patients who present to a hospital emergency department with an emergency medical condition or in labor;[27] and
- making a false record or statement material to a false or fraudulent claim for payment for items and services furnished under a Federal health care program.[28]

1. Beneficiary Inducements CMP

The Beneficiary Inducements CMP[29] provides for the imposition of CMPs against any person who offers or transfers remuneration to a Medicare or State health care program that the person knows or should know is likely to influence the beneficiary's selection of a particular

[21] Sections 1128A(a)(1)(A)–(B) of the Act, 42 U.S.C. §§ 1320a-7a(a)(1)(A)–(B); Section 1128A(a)(7) of the Act, 42 U.S.C. § 1320a-7a(a)(7).
[22] Sections 1128A(a)(1)(A)–(B) of the Act, 42 U.S.C. §§ 1320a-7a(a)(1)(A)–(B).
[23] Section 1128A(a)(6) of the Act, 42 U.S.C. § 1320a-7a(a)(6).
[24] Section 1128A(a)(1)(E) of the Act, 42 U.S.C. § 1320a-7a(a)(1)(E).
[25] Section 1128A(a)(7) of the Act, 42 U.S.C. § 1320a-7a(a)(7).
[26] Section 1128A(a)(10) of the Act, 42 U.S.C. § 1320a-7a(a)(10).
[27] Section 1867(d)(1) of the Act, 42 U.S.C. § 1395dd(d)(1).
[28] Section 1128A(a)(12) of the Act, 42 U.S.C. § 1320a-7a(a)(12).
[29] Section 1128A(a)(5) of the Act, 42 U.S.C. § 1320a-7a(a)(5).

Return to TOC

provider, practitioner, or supplier for the order or receipt of any item or service for which payment may be made, in whole or in part, by Medicare or a State health care program.

There are exceptions to the definition of "remuneration" under the Beneficiary Inducements CMP. For any applicable exception to apply, each condition of the exception must be squarely satisfied. The exceptions include, for example:

- nonroutine waivers of copayments and deductibles based on individualized determinations of financial need;
- preventive care incentives;
- items and services that promote access to care and pose a low risk of harm;
- retailer rewards; and
- items and services tied to medical care for financially needy beneficiaries.[30]

The Beneficiary Inducements CMP is distinct from the Federal anti-kickback statute and the corresponding anti-kickback CMP, but the Beneficiary Inducements CMP and Federal anti-kickback statute often prohibit overlapping conduct. The Beneficiary Inducements CMP "is a separate and distinct authority, completely independent of the [Federal] anti-kickback statute."[31] It is narrower than the Federal anti-kickback statute and the anti-kickback CMP in several ways. For example: The Federal anti-kickback statute's prohibition applies to remuneration to induce or reward, among other things, referrals of an individual *to a person for the furnishing of any item or service*, and purchases of *any good, facility, service, or item*, payable by a Federal health care program. In contrast, the prohibition under the Beneficiary Inducements CMP applies to remuneration that is likely to influence a beneficiary's selection of a *particular provider, practitioner, or supplier* for items or services reimbursable by Medicare or a State health care program. Here are some additional distinctions:

- The Beneficiary Inducements CMP applies only to the person offering or transferring the remuneration. The Federal anti-kickback statute and anti-kickback CMP apply to both the person offering or paying the remuneration and the person soliciting or receiving it.
- The Beneficiary Inducements CMP applies only to items and services reimbursable by Medicare or a State health care program (e.g., Medicaid and Children's Health Insurance Program (CHIP)). The Federal anti-kickback statute and anti-kickback CMP apply to

[30] *See* Section 1128A(i)(6) of the Act, 42 U.S.C. § 1320a-7a(i)(6); 42 C.F.R. § 1003.110 for the requirements for these exceptions as well as other exceptions.
[31] *See* Revised OIG Civil Money Penalties Resulting From the Health Insurance Portability and Accountability Act of 1996, 63 Fed. Reg. 14393, 14395 (Mar. 25, 1998).

Return to TOC

HHS Office of Inspector General

items and services payable by *any* Federal health care program (e.g., Medicare, TRICARE, and CHAMPVA) or by a State health care program.

- The Beneficiary Inducements CMP uses a definition of "remuneration" that does not apply for purposes of the Federal anti-kickback statute and the anti-kickback CMP. "Remuneration" for purposes of the Beneficiary Inducements CMP is defined as including transfers of items or services for free or for other than fair market value.[32] OIG has determined that incentives that are only nominal in value are not prohibited by the Beneficiary Inducements CMP and currently interprets "nominal in value" to mean no more than $15 per item or $75 in the aggregate on an annual basis.[33]
- The Beneficiary Inducements CMP also has exceptions to the definition of "remuneration" that do not apply for purposes of the Federal anti-kickback statute or the anti-kickback CMP.[34]

Individuals and entities should be mindful of the potential applicability of these statutes to the same or similar conduct, as well as the differences in these statutes, when conducting training, designing risk assessments, and developing and implementing policies regarding remuneration to beneficiaries.

2. Information Blocking

Pursuant to the 21st Century Cures Act, OIG has the authority to investigate claims that health information technology (IT) developers of certified health IT (including entities offering certified health IT), health information exchanges and networks, and health care providers have engaged in conduct constituting "information blocking."[35] A health IT developer of certified health IT[36] and health information exchanges and networks commit information blocking when they engage in a practice that is likely to interfere with, prevent, or materially discourage the access, exchange, or use of electronic health information (EHI) and they know, or should know, the practice is likely to interfere with, prevent, or materially discourage the access, exchange, or use of EHI. A health care provider commits information blocking when the provider engages in a practice that is likely to interfere with, prevent, or materially discourage the access, exchange, or use of EHI, and the provider knows the practice is unreasonable and is likely to interfere with, prevent, or materially discourage the access, exchange, or use of EHI. Information

[32] Section 1128A(i)(6) of the Act, 42 U.S.C. § 1320a-7a(i)(6).
[33] *See, e.g.,* Medicare and State Health Care Programs: Fraud and Abuse; Revisions to the Safe Harbors Under the Federal anti-kickback statute and Civil Monetary Penalty Rules Regarding Beneficiary Inducements, 81 Fed. Reg. 88368, 88394 (Dec. 7, 2016); Office of Inspector General Policy Statement Regarding Gifts of Nominal Value to Medicare and Medicaid Beneficiaries.
[34] Section 1128A(i)(6) of the Act, 42 U.S.C. § 1320a-7a(i)(6); 42 C.F.R. § 1003.110.
[35] Section 4004 of the 21st Century Cures Act, 42 U.S.C. § 300jj-52.
[36] This includes entities that offer certified health IT as defined in 45 C.F.R. § 171.102.

Return to TOC

blocking does not include any practice that is required by law or that meets an exception. The Office of the National Coordinator for Health Information Technology (ONC) has promulgated regulations setting forth important definitions and exceptions,[37] and has also issued several guidance documents.[38] It is important to understand that ONC's regulations define the conduct that constitutes information blocking.

The penalties for engaging in information blocking depend on the type of individual or entity. A health IT developer of certified health IT, health information exchange, or network that engages in information blocking may be subject to CMPs of up to $1 million per violation. OIG has issued a Final Rule[39] on its investigations of and the imposition of CMPs on health IT developers of certified health IT (which includes entities that offer health IT), health information exchanges, and health information networks. A health care provider may be subject to the appropriate disincentives as set forth by HHS in a future rulemaking.[40] Individuals and entities that meet the definition of health care provider under ONC's regulations should be mindful that they may be subject to CMPs if they meet the definition of health IT developers of certified health IT or health information exchanges and networks under ONC's regulations.[41]

3. CMP Authority Related to HHS Grants, Contracts, and Other Agreements

OIG has the authority to impose CMPs, assessments, and exclusion against individuals or entities that engage in a variety of fraudulent and other improper conduct related to HHS grants, contracts, and other agreements.[42] For instance, OIG may pursue individuals or entities that, with regard to HHS grants, contracts, or other agreements:

- present a false or fraudulent specified claim;
- make a false statement or omission;
- make or use a false record;
- conceal or improperly avoid an obligation owed to HHS; or
- fail to grant access to OIG for the purpose of audits, investigations, or evaluations.

---

[37] 45 C.F.R. part 171.
[38] *See* ONC Information Blocking Resources; OIG Information Blocking Resources.
[39] OIG Information Blocking Final Rule, 88 Fed. Reg. 42820 (July 3, 2023); 42 C.F.R. § 1003.1400.
[40] At the time of publication of the GCPG, HHS has a pending rulemaking in the Unified Agenda at Regulation Identifier No. 0955-AA05.
[41] This is discussed both in ONC's rule and in OIG's rule.
[42] Section 1128A(o) of the Act, 42 U.S.C. § 1320a-7a(o).

Return to TOC

Here is an example of conduct that would create grant fraud CMP liability:

> A grantee was awarded HHS grant funds for the purposes of paying for substance use disorder treatment services to members of a local community. Instead of limiting use of the funds for such treatment services, the grantee knowingly used the funds to also pay for prohibited expenses, such as the clients' rent, mortgage, utilities, and auto repairs.

It is important for HHS awardees to understand what conduct leads to liability under OIG's authority, as well as under other fraud and abuse laws, and to put internal controls into place to prevent and identify these issues early.

More information about fraud areas of concern related to grants, contracts, and other agreements is available here. In addition, self-disclosure information specific to HHS grants and contracts are discussed in section VI.G, OIG Self-Disclosure Information.

E. Exclusion Authorities

OIG has the legal authority to exclude individuals and entities from participation in all Federal health care programs under section 1128 of the Act (42 U.S.C. § 1320a-7). Federal health care programs include all plans and programs that provide health benefits funded directly or indirectly by the United States (except for the Federal Employees Health Benefits Program) or any State health care program.[43] State health care programs include State Medicaid programs, the Maternal and Child Health Services Block Grant program under Title V of the Act, Block Grants to States for Social Services under subtitle A of Title XX of the Act, and the Children's Health Insurance Program under Title XXI.[44] OIG maintains a list of all currently excluded individuals and entities called the List of Excluded Individuals/Entities (LEIE). Information about the LEIE may be found on the OIG's Exclusions Page.

Mandatory Exclusions

OIG is *required* by law to exclude from participation in all Federal health care programs individuals and entities convicted of certain types of criminal offenses, including:

- offenses related to the delivery of an item or service under Medicare or a State health care program;

[43] Section 1128B(f) of the Act, 42 U.S.C. § 1320a-7b(f).
[44] Section 1128(h) of the Act, 42 U.S.C. 1320a-7(h).

Return to TOC

- patient abuse or neglect;
- felony convictions for other health care-related fraud, theft, embezzlement, breach of fiduciary responsibility, or other financial misconduct; and
- felony convictions relating to the unlawful manufacture, distribution, prescription, or dispensing of controlled substances.[45]

Permissive Exclusions

OIG has *discretion* to exclude individuals and entities on a number of grounds, including (but not limited to):

- misdemeanor convictions related to health care fraud not involving Medicare or a State health program;
- fraud in a program (other than a health care program) funded by any Federal, State, or local government agency;
- misdemeanor convictions relating to the unlawful manufacture, distribution, prescription, or dispensing of controlled substances;
- suspension, revocation, or surrender of a license to provide health care for reasons bearing on professional competence, professional performance, or financial integrity;
- provision of unnecessary or substandard services;
- submission of false or fraudulent claims to a Federal health care program;
- engaging in arrangements that violate the Federal anti-kickback statute;
- defaulting on health education loan or scholarship obligations; and
- controlling a sanctioned entity as an owner, officer, or managing employee.[46]

The effect of an OIG exclusion is that no Federal health care program payment may be made for any items or services furnished: (1) by an excluded person, or (2) at the medical direction or on the prescription of an excluded person.[47] Payment for claims submitted to a Federal health care program for items or services furnished by an excluded individual or entity results in an overpayment, regardless of whether the excluded individual had a provider identification number and the ability to bill separately.[48]

OIG has the legal authority to impose CMPs on individuals and entities that arrange or contract (by employment or otherwise) with an individual or entity that the person knows or should

[45] Section 1128(a) of the Act, 42 U.S.C. § 1320a-7(a).
[46] Section 1128(b) of the Act, 42 U.S.C. § 1320a-7(b).
[47] 42 C.F.R. § 1001.1901.
[48] *See, e.g.,* Section 1128J(d) of the Act, 42 U.S.C. § 1320a-7k(d).

Return to TOC

know is excluded from participation in a Federal health care program for the purpose of providing items and services for which payment may be made by a Federal health care program.[49] OIG may impose penalties for each item or service furnished by the excluded individual or entity for which a claim was submitted to a Federal health care program.

OIG recommends that employers study the resources provided on OIG's website to fully understand the effects of exclusion.

Many providers and their staff employ excluded individuals because they incorrectly believe it is permissible (for example, because an employee obtains a new health care license or has received permission from a State agency to practice, has an administrative role, cannot separately bill).

Some of these resources can be found at the following links: Updated Special Advisory Bulletin on the Effect of Exclusion on Participation in the Federal Health Care Programs and Frequently Asked Questions.

To avoid overpayment and CMP liability, entities participating in Federal health care programs should check the LEIE before employing or contracting with individuals and entities, and periodically check the LEIE to determine the exclusion status of current employees and contractors. The LEIE is a tool that OIG has made available to providers and others to enable them to identify potential and current employees or contractors that are excluded by OIG.

If an entity discovers that it has employed or contracted with an excluded individual or entity, the entity should evaluate its overpayment and CMP liability. We recommend that entities in this situation consider whether to submit a self-disclosure through the Health Care Fraud Self-Disclosure Protocol.

OIG updates the LEIE monthly, so screening each month best minimizes potential overpayment and CMP liability.

Many State Medicaid programs now have their own exclusion authorities and maintain their own State exclusion lists. If an entity employs or contracts or otherwise engages with individuals or entities excluded from a State Medicaid program in which it participates, the

[49] Section 1128A(a)(6) of the Act, 42 U.S.C. § 1320a-7a(a)(6).

Return to TOC

27

entity may incur overpayment liability. It may also incur CMP liability. OIG recommends that entities check employees, contractors, and other individuals or entities that provide items and services that may be paid for by the State Medicaid programs in which they participate against such State Medicaid program exclusion lists.

For example, if an entity has a hospital in Illinois that participates in the Illinois and Iowa state Medicaid programs, OIG recommends that the entity screen all employees and contractors who provide items or services at the facility, or who provide support to the facility, against both the Illinois and Iowa state Medicaid exclusion lists.

F. Criminal Health Care Fraud Statute

There is a criminal health care fraud statute that makes it a criminal offense to defraud a health care benefits program. The criminal health care fraud statute prohibits knowingly and willfully executing, or attempting to execute, a scheme to either: (1) defraud any health care benefit program; or (2) to obtain, by means of false or fraudulent pretenses, representations, or promises, any money or property from any health care benefit program.[50] The Government must prove its case beyond a reasonable doubt and prove that the defendant acted with intent to defraud; however, specific intent to violate this statute is not required for a conviction. DOJ, OIG, and other law enforcement partners have successfully used this statute to pursue defendants who orchestrate complex health care fraud schemes. Cases that involve violations of the criminal health care fraud statute also often involve complex money laundering, tax, and other associated financial criminal offenses. The penalties for violating the criminal health care fraud statute may include fines of up to $250,000, imprisonment of not more than 10 years, or both.

G. HIPAA Privacy and Security Rules

HHS's OCR is responsible for administering and enforcing the HIPAA Privacy, Security, and Breach Notification Rules. The Standards for Privacy of Individually Identifiable Health Information, known as the Privacy Rule, addresses the use and disclosure of individuals' identifiable health information (protected health information or PHI) by covered entities,[51] including health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically, and their business associates.[52, 53] The Privacy Rule requires appropriate safeguards to protect the privacy of PHI and sets limits and conditions on the uses and disclosures that may be made of such information without an individual's authorization. The Privacy Rule also gives individuals rights over their protected health information, including rights to examine and obtain a copy of their health records, to direct a covered entity to transmit to a third party an electronic copy of their protected health information in an electronic health record, and to request corrections.

---

[50] 18 U.S.C. § 1347.

[51] The definition of "covered entity" is available at 45 C.F.R. § 160.103. CMS offers a Covered Entity Decision Tool to help entities determine if they are a covered entity.

[52] The definition of "business associate" is available at 45 C.F.R. § 160.103.

[53] 45 C.F.R. parts 160 and 164, subparts A and E.

Return to TOC

29

Tip **An entity regulated by Privacy Rule requirements should ensure that it is compliant with all applicable provisions of the Privacy Rule, including provisions pertaining to required disclosures (and permitted uses and disclosures), when developing its privacy procedures that are tailored to fit the entity's particular size and needs.**

The Security Standards for the Protection of Electronic Protected Health Information, known as the Security Rule,[54] was also promulgated pursuant to HIPAA. It specifies a series of administrative, physical, and technical safeguards for covered entities and their business associates to ensure, among other provisions, the confidentiality, integrity, and security of electronic PHI. Covered entities and their business associates can consider their organization and capabilities, as well as costs, in designing their security plans and procedures to comply with Security Rule requirements. Notably, OCR and ONC jointly launched a HIPAA Security Risk Assessment Tool. The tool's features make it useful in assisting small and medium-sized health care practices and business associates as they perform a risk assessment. Also, the National Institute of Standards and Technology (NIST) developed the NIST HSR Toolkit, which is a self-assessment survey intended to help organizations better understand the requirements of the Security Rule, implement those requirements, and assess those implementations in their operational environment.

The Notification in the Case of Breach of Unsecured Protected Health Information, known as the Breach Notification Rule,[55] was promulgated pursuant to the Health Information Technology for Economic and Clinical Health Act, passed as part of American Recovery and Reinvestment Act of 2009. The Breach Notification Rule requires covered entities and their business associates to provide notification following a breach of unsecured PHI. A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the PHI. Covered entities and business associates must only provide the required notifications if the breach involved unsecured PHI. Unsecured PHI is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance.

[54] 45 CFR parts 160 and 164, subparts A and C.
[55] 45 CFR parts 160 and 164, subparts A and D.

Return to TOC

30

The statutory and regulatory background for the Privacy, Security, and Breach Notification Rules[56] can be found on HHS's website. A wealth of other resources, including FAQs and information specific to compliance and enforcement, is also publicly available on the website.

With increasing numbers of cybersecurity attacks aimed at HIPAA-regulated entities of all sizes, compliance with Privacy, Security, and Breach Notification Rule requirements should be a top compliance priority and included in all risk assessments.

[56] 45 CFR Parts 160 and 164, subparts A and E.

SECTION III
Compliance Program Infrastructure: The Seven Elements

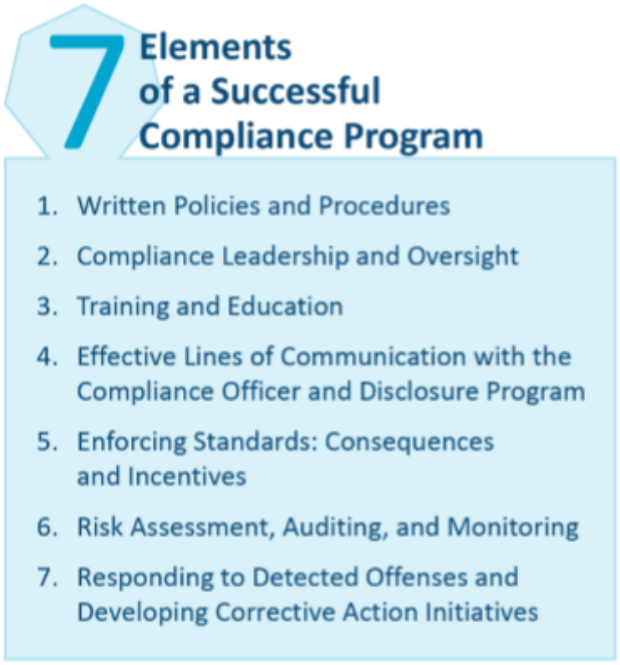
Return to TOC

HHS Office of Inspector General

32

III. Compliance Program Infrastructure: The Seven Elements

In this section, we discuss the seven elements of an effective compliance program. Acknowledging the broad spectrum of entities playing a role in health care delivery today, our discussion below provides guidance generally applicable across the entire spectrum. **We discuss modifications small entities may use to implement these sections in** section IV.A.



Our guidance in this section reflects our prior guidance; more than 25 years of experience monitoring Corporate Integrity Agreements (CIAs); feedback received in various forms from industry stakeholders; lessons learned from enforcement actions and investigations; and the ongoing evolution of the health care delivery system and technology used to support that delivery system.

OIG's longstanding belief is that an entity's leadership should commit to implementing all seven elements to achieve a successful compliance program. The guidance in this section is intended to help entities fulfill that commitment in a robust and meaningful way.

Return to TOC

HHS Office of Inspector General

33

Element 1—Written Policies and Procedures

Generally, health care entities instruct their employees, contractors, and medical staff on certain duties and any standard parameters around the performance of such duties through policies and procedures. More specifically, through written policies and procedures, entities can provide a roadmap for **relevant individuals**, outlining their duties within the organization, developing workflow management, imposing documentation requirements, defining individual and organizational oversight roles, and implementing controls entity-wide to mitigate compliance risks specific to the entity. Policies and procedures also demonstrate to stakeholders and other interested parties, including Government regulators, how the entity strives to comply with applicable laws, regulations, and requirements.

A code of conduct and compliance policies are critical elements of any compliance program. The compliance program should also require that all the entity's policies and procedures incorporate a culture of compliance into its day-to-day operations. The code of conduct and compliance policies and procedures should be developed under the direction and supervision of the compliance officer and the Compliance Committee and should be made available to all relevant individuals within the organization. Compliance with the code of conduct and applicable policies and procedures should be part of the performance evaluations of all employees and contractors.

1. Code of Conduct

A code of conduct is an important tool to communicate an organization's mission, goals, and ethical requirements central to its operations. The code articulates the entity's commitment to comply with all Federal and State laws and regulations. It defines the entity's ethical standards necessary to fulfill its mission and govern the conduct of its officers, employees, contractors, medical staff, and others who work with or on behalf of the organization.

CEOs can demonstrate their embrace of the organization's commitment to compliance with a signed introduction in the code. To demonstrate broader organizational commitment to compliance, the board also may wish to include a signed endorsement or a similar written statement.

Although the code by its design may not need regular review, any handbook delineating or expanding upon the code of conduct should be regularly updated as applicable statutes, regulations, and Federal health care program requirements change.

Return to TOC

HHS Office of Inspector General

Entities may wish to review their codes when a new CEO is hired, particularly if the code contains a letter, quotations, or other endorsements by the preceding CEO. Leadership change provides an opportunity for the entity to ensure that its code reflects the entity's ongoing commitment to compliance.

2. Compliance Policies and Procedures

Compliance policies and procedures should encompass at least two areas: (1) the implementation and operation of the entity's compliance program, including the seven elements discussed in this section; and (2) processes to reduce risks caused by noncompliance with Federal and State laws. **A discussion of Federal fraud and abuse authorities is included in Section II above.** Entities should assess how their operations may present risk areas specific to them and design policies and procedures that address these risks.

Some common compliance risk areas are:

- billing;
- coding;
- sales;
- marketing;
- quality of care;
- patient incentives; and
- arrangements with physicians, other health care providers, vendors, and other potential sources or recipients of referrals of health care business.

OIG recommends that entities review the current health care subsector Compliance Program Guidance on the OIG website for a further discussion of subsector-specific risks.

The Compliance Committee should ensure that a system exists to ensure that the entity's policies and procedures foster rather than undermine the entity's compliance culture. When the entity creates, revises, or deletes a policy, it should consider whether the change affects the entity's compliance with government health care program requirements, encourages or incentivizes noncompliance, or impairs the entity's risk-mitigation efforts.

Return to TOC

HHS Office of Inspector General

35

All organizations should have a policy and procedure on the screening of employees, contractors, and other individuals and entities that furnish items and services for or on behalf of the organization against the LEIE and any applicable State Medicaid program exclusion lists. The policy should clearly identify which individual(s) in the organization are responsible for conducting the screening, the process for performing the screening and verifying any potential matches, and the steps that should be taken in the event an entity learns that an individual or entity that has been excluded by the OIG or a State Medicaid program. More information on screening may be found in the Updated Special Advisory Bulletin on the Effect of Exclusion From Participation in Federal Health Care Programs.

Entities may choose to rely on screening conducted by a contractor (e.g., staffing agency, physician group, or third-party billing or coding company), but OIG recommends that entities validate that the contractor is conducting such screening on behalf of the provider (e.g., by requesting and maintaining screening documentation from the contractor). The entity remains responsible for any overpayment or CMP liability that may result from employing or contracting with an excluded individual or entity in a manner that violates the exclusions authorities.

Policy Maintenance

All **relevant individuals** should be able to easily access their organization's code, policies, and procedures. Many entities now maintain their code, policies, and procedures on an internal intranet site or use other electronic communication tools to ensure that everyone has access to the same documents. If the entity's communication method does not provide access to all relevant individuals, the entity should employ an alternative mechanism for such individuals to obtain access to the code, policies, and procedures. Besides being accessible, the code, policies, and procedures also should be comprehensible by all relevant individuals (e.g., translated into other languages, where appropriate, and written at appropriate reading levels).

Return to TOC

HHS Office of Inspector General

36

The organization's compliance officer should ensure that compliance policies and procedures are effectively created, coordinated, and maintained.

DOJ has compiled a useful set of questions for entities to consider in setting up and reviewing their system of policies and procedures. These may be found at DOJ Evaluation of Corporate Compliance Programs.

The OIG's toolkit on Measuring Compliance Program Effectiveness also provides useful tools for evaluating policies and procedures, as well as identifying gaps that may require new or revised policies and procedures. It may be found on the OIG's Compliance Toolkits page.

Entities should set up a regular schedule for reviewing and revising, as necessary, all policies and procedures. OIG recommends that entities review policies and procedures at least annually to ensure that such policies and procedures reflect any modifications to applicable statutes, regulations, and Federal health care program requirements.

Up-to-date policies and procedures are a critical element of a compliance program. Entities should ensure that they finalize and make available to **relevant individuals** any new or revised policies and procedures before implementing or altering practices and processes. The entity's employees, contractors, and other relevant individuals should be able to rely on an entity's policies and procedures as the entity's current instructions on a particular subject. Having policy and procedure documents that are not up to date diminishes their credibility to the users of such policies and procedures and other interested parties, including Government regulators. Inaccurate or unreliable policies and procedures also reduce the compliance program's authority, credibility, and effectiveness at the entity.

Who is a relevant individual?

For the purposes of this GCPG, a "relevant individual" means a person whose responsibilities or activities are within the scope of the code, policy, or procedure. Relevant individuals could include employees, contractors, patients, customers, agency staff, medical staff, subcontractors, agents, or people in other roles, or a subset of the above. Each entity needs to determine for itself who their relevant individuals are."

OIG encourages entities to include in their disclosure program **(discussed further in** section III.D **below)** a means for employees, contractors, and other relevant individuals to contact the

Return to TOC

HHS Office of Inspector General

compliance officer or members of the Compliance Committee with questions about a policy or procedure.

Tip **If the procedure for policy revision and approval impedes rapid implementation of a needed process change, OIG recommends that the entity devise a means of communicating and documenting interim policies and procedures to the relevant impacted individuals.**

B. Element 2—Compliance Leadership and Oversight

Boards and **senior leadership** are vital to effective compliance programs. An effective compliance program reduces and mitigates risk, provides patients safe and high-quality care, and saves costs. To be effective, a compliance program should have a board and senior leadership that understand its value and are committed to its success. One of these senior leaders should be the Compliance Officer.

Senior Leadership

For the purposes of the GCPG, "senior leadership" means the group of leaders who report directly to the executive leading the entity, usually the CEO. Some entities refer to this group by other names, such as executive leadership.

1. Compliance Officer

Every entity should designate a leader as the entity's compliance officer. A key indicator of the board and senior leadership's commitment to compliance is the appointment and support of a compliance officer who has the authority, stature, access, and resources necessary to lead an effective and successful compliance program. Designating a compliance officer with appropriate authority is essential to the success of the compliance program.

The compliance officer should:

- report either to the CEO with direct and independent access to the board[57] or to the board directly;
- have sufficient stature within the entity to interact as an equal of other senior leaders of the entity;

Return to TOC

HHS Office of Inspector General

- demonstrate unimpeachable integrity, good judgment, assertiveness, an approachable demeanor, and the ability to elicit the respect and trust of entity employees; and
- have sufficient funding, resources, and staff to operate a compliance program capable of identifying, preventing, mitigating, and remediating the entity's compliance risks.

The Compliance Officer's Primary Responsibilities

These should include:

- overseeing and monitoring the implementation and operation of the compliance program;
- advising the CEO, board, and other **senior leaders** on compliance risks facing the entity, compliance risks related to strategic and operational decisions of the entity, and the operation of the entity's compliance program;
- chairing the Compliance Committee;
- reporting to the board on the implementation, operation, and needs of the compliance program, the compliance risks the entity faces, and the methods through which the entity is addressing or can address those risks;
- revising the compliance program periodically in light of changes in the needs of the organization, applicable law, and policies and procedures of third-party payors;
- coordinating with Human Resources to ensure that all directors, officers, employees, contractors, and medical staff, if applicable, are screened before appointment or engagement and monthly thereafter against the LEIE and any applicable State Medicaid program exclusion lists;

The Compliance Officer's primary responsibilities should include advising the CEO, board, and other senior leaders on compliance risks facing the entity, compliance risks related to strategic and operational decisions of the entity, and the operation of the entity's compliance program.

Return to TOC

HHS Office of Inspector General

39

- coordinating with other relevant entity components (e.g., as applicable, Internal Audit, Risk, **Quality**, IT) to develop work plans for reviewing, monitoring, and auditing compliance risks;
- independently investigating and acting on matters related to compliance, including the flexibility to design and coordinate internal investigations (e.g., responding to reports involving, for example, compliance concerns or suspected legal violations) and to make recommendations for process and policy changes and corrective action; and
- developing policies and programs that encourage personnel to report suspected fraud and other improprieties without fear of retaliation.

Quality

For the purposes of this GCPG, "quality" means both quality in manufacturing and supplying drugs, devices, and other items, and quality of care in the provision of items and services.

To fulfill their duties, the compliance officer should be empowered, and independent of other duties to the entity that might impair their ability, to identify and raise compliance risks and advise on how to mitigate risks, achieve and maintain compliance with Federal health care program requirements, and succeed as a compliant entity. **Thus, the compliance officer should not lead or report to the entity's legal or financial functions, and should not provide the entity with legal or financial advice or supervise anyone who does. The compliance officer should report directly to the CEO or the board. Usually, leaders of these functions are the general counsel and the chief financial officer, but some entities give them different titles.**

To be effective, the compliance officer should also maintain a degree of separation from the entity's delivery of health care items and services and related operations. Thus, the compliance officer should not be responsible, either directly or indirectly, for the delivery of health care items and services or billing, coding, or claim submission. In addition, involvement in functions such as contracting, medical review, or administrative appeals present potential conflicts. Whenever possible, the compliance officer's sole responsibility should be compliance.

Tip

Some compliance officers have the dual role of privacy officer. In that case, OIG recommends that the entity ensure that the compliance officer has sufficient staff and resources to perform the additional duties associated with that expanded role.

Return to TOC

HHS Office of Inspector General

Coordination and communication are the compliance officer's key tools for planning, implementing, and monitoring an effective compliance program. The compliance officer should strive to develop, and the entity should strive to promote, productive working relationships with organizational leaders. Coordinating work and sharing information with leaders of other support functions, including (as applicable), Legal, Internal Audit, IT and Health Information Management (HIM), Human Resources, **Quality**, Risk Management, and Security will enhance the strength and success of the compliance program.

The compliance officer should have the authority to review all documents, data, and other information that are relevant to the organization's compliance activities. This includes, but is not limited to, patient records, billing records, sales and marketing records, and records concerning the entity's arrangements with other parties, including employees, independent contractors, suppliers, physicians, and other health care professionals. The compliance officer also should have the authority to interview anyone within or connected to the organization in connection with a compliance investigation, or designate an appropriate person to conduct such an interview.

2. Compliance Committee

The Compliance Committee's purpose is to aid and support the compliance officer in implementing, operating, and monitoring the Compliance Program. The Compliance Committee should meet no less than quarterly. Having a regularly scheduled meeting may enhance routine attendance.

The Compliance Committee's Primary Duties

These should include:

- analyzing the legal and regulatory requirements applicable to the entity;
- assessing, developing, and regularly reviewing policies and procedures;
- monitoring and recommending internal systems and controls;
- assessing education and training needs and effectiveness, and regularly reviewing required training;

Return to TOC

HHS Office of Inspector General

- developing a disclosure program and promoting compliance reporting;
- assessing effectiveness of the disclosure program and other reporting mechanisms;
- conducting annual risk assessments;
- developing the compliance workplan;
- evaluating the effectiveness of the compliance workplan and any action plans for risk remediation; and
- evaluating the effectiveness of the compliance program.

The compliance officer should be the chair of the Compliance Committee. The Compliance Committee should be comprised of the relevant leaders of both operational and supporting departments, which could include Billing and Coding, Clinical and Medical, Finance, Internal Audit, IT, HIM, Human Resources, Legal, **Quality**, Risk Management, Sales and Marketing, and other operational managers. All members should be sufficiently knowledgeable regarding their department's subject area. All members should have the authority and ability to speak for the department they represent.

Before joining the Compliance Committee, provide training to the new member on the committee's duties and responsibilities and the entity's expectations of them in their role as a committee member.

Actively leading the Compliance Committee and its meetings is an important and integral function of the compliance officer. As the Compliance Committee chair, the compliance officer should establish and facilitate committee discussion and encourage active participation by all committee members.

Circulating an agenda before the meeting will inform members of the meeting topics and give them an opportunity to prepare.

The compliance officer should assist with the identification of risk areas and monitor and report on progress toward committee objectives. The compliance officer should mediate any disagreement between or among committee members and escalate committee matters that remain unresolved to the CEO. Throughout each meeting of the Compliance Committee, the compliance officer should continue to focus the committee's attention on compliance program effectiveness and the benefits of an effective compliance program to the organization.

Return to TOC

HHS Office of Inspector General

Tip **Keeping minutes of Compliance Committee meetings will provide a documentary record of the Committee's activities and accomplishments.**

The tone for all aspects of the Compliance Program, including the Compliance Committee, should be established and maintained by an organization's leadership, including the board and the CEO. Expectations for regular, diligent member attendance at Compliance Committee meetings should be set by the board and enforced by the CEO. Member attendance, active participation, and contributions should be included in each member's performance plan and compensation evaluation. In their communications with individual committee members, the board and the CEO should regularly convey the importance of, and their interest in, the member's Compliance Committee responsibilities and participation.

Member attendance, active participation, and contributions should be included in each member's performance plan and compensation evaluation.

The compliance officer should periodically provide a report to the board assessing the Compliance Committee's performance. This report should compare the entity's expectations of the committee's performance with its actual performance. As part of the assessment, the compliance officer should seek input from the members of the Compliance Committee, the CEO, and the board. The compliance officer also should examine how the entity implemented committee decisions and recommendations.

Return to TOC

Indicators of Committee Success

- substantive committee discussions;
- active engagement by committee members;
- demonstrations of authority and autonomy (within the scope of the Compliance Committee's charter);
- accountability and follow-through of committee determinations;
- establishment of a robust, detailed work plan;
- and mitigation of compliance risks.

In their report to the board, the compliance officer should include any recommendations they may have on adjustments to improve the Compliance Committee's performance. Adjustments could include revisions to committee charter, scope, or membership, expectations regarding membership, and methods of ensuring committee and member accountability.

3. Board Compliance Oversight

The United States Sentencing Commission's Guidelines require that an entity's "governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program."[58]

Boards should pay attention to the Commission's Guidelines because federal courts consult when determining criminal sentences. Corporate boards also have a fiduciary duty of care, which requires that boards assure that "information and reporting systems exist in the organization that are reasonably designed to provide to senior management and to the board itself timely, accurate information to allow management and the board, each within its scope, to reach informed judgments concerning … the

[58] United States Sentencing Commission, Guidelines Manual, § 3E1.1 (Nov. 2021)

Return to TOC

HHS Office of Inspector General

corporation's compliance with the law . . . . " In re Caremark, 698 A.2d 959, 970 (Del. Ch. 1996).

The board's exercise of this responsibility should include overseeing the compliance officer and the Compliance Committee and receiving and reviewing information necessary to understand the entity's compliance risks. The board also should have access to sufficient knowledge and resources to allow it to fulfill its compliance-related obligations competently.Oversight of the compliance officer is a critical component of the board's compliance role. The board should ensure that the compliance officer has sufficient power, independence, and resources to implement, maintain, and monitor the entity's compliance program and advise the board about the entity's compliance operations and risk.

The board should ensure that the compliance officer has sufficient power, independence, and resources to implement, maintain, and monitor the entity's compliance program and advise the board about the entity's compliance operations and risk.

To ensure the compliance officer is sufficiently empowered, the board should assure that the compliance officer's stature is commensurate with their responsibilities and those of other entity **senior leaders** and that the organization is structured to permit the compliance officer to inform the board of challenging compliance risks without fear of personal or financial repercussions. Regardless of the reporting structure, the board should also ensure that the compliance officer has direct and uninhibited access to the board at any time.

To ensure the compliance officer's independence, the board should determine that the compliance officer is free of organizational responsibilities that would impede the compliance officer's ability to evaluate and report on compliance risk. The Compliance Officer section **discusses roles and responsibilities for which the compliance officer should not be responsible.** The board also should regularly review whether the compliance officer and the compliance program have sufficient staff and resources for an entity of its size, complexity, and interaction with Federal health care programs.

The board should meet with the compliance officer on a regular basis and no less than quarterly. The compliance officer should provide the board with regular reports regarding the entity's compliance program, activities, and risks, and participate in an oral discussion of the report with board members. The board should reserve time at each session for an executive

Return to TOC

HHS Office of Inspector General

meeting with the compliance officer, without non-board members present, to permit the board and the compliance officer to have an uninhibited discussion of compliance risks of concern, including the adequacy of compliance staff and resources.

As OIG has stated in the Practical Guidance for Health Care Boards on Compliance Oversight, "[s]cheduling regular executive sessions creates a continuous expectation of open dialogue, rather than calling such a session only when a problem arises, and is helpful to avoid suspicion among management about why a special executive session is being called."

Another important component of the board's compliance role is Compliance Committee oversight. The board should ensure that: (1) the Compliance Committee fully understands and exercises its role, (2) the Compliance Committee's decisions and activities are appropriately implemented and performed, and (3) the board understands and evaluates how the Compliance Committee addresses risk. Compliance Committee members sometimes mistakenly see their role as overseeing the compliance officer and the compliance program, rather than supporting and working with the compliance officer on the compliance program. Boards should strive to ensure that Compliance Committee members correctly understand their role.

The Compliance Committee should provide the board with regular reports on member attendance and the board should ensure that the CEO enforces accountability. The board should also assure that Compliance Committee members' role and performance on the committee are reflected in their performance plans and considered in compensation and promotion decisions.

> **The board should take every opportunity to communicate to each of its audiences its commitment to compliance. Every board has a variety of audiences, which could include entity leaders, personnel, individual owners, shareholders, customers, patients, payors, Federal and State Governments, and the public.**

The board should encourage the Compliance Officer and other **senior leaders** to report on how Committee decisions are implemented and supported by leaders throughout the organization. The board also should ensure that it understands how the Compliance Committee identifies and addresses risks, including health care compliance risks and any other risks that impact the entity's direct or indirect interaction with Federal health care programs and beneficiaries (e.g., privacy, **quality**, IT, data). It should receive, at least annually, reports on the entity's

Return to TOC

HHS Office of Inspector General

effectiveness in addressing and resolving committee-identified risks. The board also should periodically evaluate the effectiveness of the Compliance Committee's risk assessment process.

Tip

Although it was written before OIG began recommending that the Compliance Committee be responsible for the risk assessment and internal review process, the Measuring Compliance Effectiveness Toolkit, which may be accessed here, provides useful tips on evaluating the effectiveness of the risk assessment process.

The Practical Guidance for Health Care Boards on Compliance Oversight provides specific suggestions for how boards can effectively exercise their oversight role.

C. Element 3—Training and Education

Providing appropriate education and training is a vital component of an effective compliance program. The compliance officer, with the support and aid of the Compliance Committee, should develop and coordinate a multifaceted education and training program specific to the needs of and risks presented by the entity. The program should include education and training on the entity's compliance program, Federal and State standards applicable to the entity, and board governance and oversight of a health care entity.

The compliance officer should develop an annual training plan that includes the training topics to be delivered and the target audience for each topic. The annual training plan should incorporate material addressing any concerns identified in audits and investigations. The Compliance Committee should review the training plan at least annually to ensure that compliance training topics and materials address current needs, including any issues identified through monitoring and auditing and changes to Federal and State health care requirements.

> **All board members, officers, employees, contractors, and medical staff (if applicable) of the entity should receive training at least annually on the entity's compliance program and potential compliance risks.**

The training should describe the entity's commitment to complying with Federal and State standards and review the applicable fraud and abuse laws (e.g., the Federal False Claims Act, the Federal anti-kickback statute, PSL, and any applicable State fraud and abuse laws). This training also should explain the elements of the entity's compliance program.

Return to TOC

HHS Office of Inspector General

47

Specific topics should include, for example:

- the identity and role of the compliance officer;
- the role of the Compliance Committee;
- the importance of open communication with the compliance officer;
- the various ways individuals can raise compliance questions and concerns with the compliance officer;
- nonretaliation for disclosing or raising compliance concerns; and
- the means through which the entity enforces its written policies and procedures equitably and impartially.

An entity also may develop and require trainings reflective of risks specific to the entity's business, role in the health care delivery system, or any risks revealed through prior investigations or audits.

Targeted training sessions should be developed and assigned based on individuals' roles and responsibilities and any compliance risks specific to those roles and responsibilities. These training sessions should address Federal health care program rules applicable to the entity's business. The training sessions should cover any compliance risks specific to the learners' roles and responsibilities. Depending on the learners' roles, these may include, for example, **billing, coding, documentation, medical necessity, beneficiary inducements, gifts, interactions with physicians and other sources or recipients of referrals of Federal health care program business, and sales and marketing practices.** The education and training program also should include a requirement that licensed personnel must complete all education and training mandated by the licensing board that governs their license.

Targeted training also should be developed for board members. New board members should receive training on their governance and compliance oversight roles promptly after joining the board. The initial board training should address the specific responsibilities of health care board members, including the risks, oversight areas, and approaches to conducting effective oversight of a health care entity. The compliance officer should consider arranging additional, periodic training to update the board on the entity's compliance risks, including changes to applicable Federal and State health care requirements.

Return to TOC

HHS Office of Inspector General

An entity may choose to develop its own training materials, purchase training materials from a third-party vendor, or contract with an external party to develop the training materials. The Compliance Committee should ensure that the training materials, whether developed internally or purchased externally, appropriately address the entity's compliance program and specific compliance risks.[59]

The Compliance Committee should also ensure that the training materials are accessible to all members of the designated audience. For example, if an entity has a culturally diverse staff, training materials may need to be available in several languages. Training may be provided in many formats—live (in-person or via videoconference), a computer-based training, or through watching a pre-recorded video. Regardless of the format, the Compliance Committee should ensure that there is a mechanism for participants to ask questions about the content. For example, the training materials could encourage individuals to submit questions to the compliance officer via email.

The entity may incorporate a process through which contracting entities' employees may receive a training waiver by demonstrating that the contracting entity's compliance training and education program satisfies certain requirements. The compliance officer should ensure that outside contractors receiving any such waiver inform its employees of the entity's disclosure program and the ways in which the contractor's employees may report compliance concerns to the entity directly.

Participation in required compliance training programs should be made a condition of continued employment or engagement by the entity. Failure to comply with training requirements should result in consequences, up to and including possible termination of employment or engagement when warranted by the circumstances. Completion of mandatory training should be a basic requirement of each employee's annual performance evaluation. Completion of mandatory training should also be a required component of evaluation of contractors. Hospitals and other entities with medical staff should work closely with their chief medical officers and chiefs of staff to ensure all members of the medical staff complete required compliance training.

Education should not be limited to annual formal training requirements. The compliance officer should seek and develop opportunities to provide education on compliance topics and risks throughout the year.

[59] For example, a compliance training course developed for hospitals would not be applicable to a home health agency.

Return to TOC

HHS Office of Inspector General

49

Some ideas to provide compliance-related education include:

- developing and updating FAQs on the entity's electronic communication site or on posters in employee common areas;
- having a standing compliance item on the agenda for regularly scheduled meetings;
- writing a regular column in the entity's newsletter;
- posting video clips;
- participating in the annual sales meeting;
- occasionally dropping in on an informal morning huddle; and
- walking the floors.

The compliance officer also should consider working with the Compliance Committee to have various committee members and entity leaders deliver compliance training in meetings and settings where they already appear. This will help normalize compliance as an integral part of the entity's culture.

Having a standing compliance item on the agenda of regular meetings is an excellent way to share information and underscore the entity's commitment to compliance. For example, this could include executive leadership meetings, entity all-hands meetings, and medical staff meetings.

Return to TOC

HHS Office of Inspector General

50

D. Element 4—Effective Lines of Communication with the Compliance Officer and Disclosure Programs

An open line of communication between the compliance officer and entity personnel (including contractors and agents) is critical to the successful implementation of a compliance program and the reduction of any potential for fraud, waste, and abuse. Entity personnel should be informed about the ways they can reach the compliance officer directly (e.g., via email, telephone, messaging). This information also should be posted in commonly frequented physical and virtual spaces. The compliance officer may wish to occasionally poll entity personnel on means of reaching the compliance officer to ensure that diverse personnel (including personnel of different generations and communication preferences) have familiar means of communicating with the compliance officer.

Entity personnel should be encouraged to bring compliance questions to the compliance officer. Such questions can be a useful source of information for the compliance officer and may help:

- create ideas for new FAQs;
- evaluate the effectiveness of training and compliance messaging;
- determine whether policy or process changes may be needed; and
- identify potential compliance risks.

Written confidentiality and nonretaliation policies should be developed and distributed to all employees to encourage communication with the compliance officer and the reporting of incidents of potential fraud and other compliance concerns.

OIG believes that whistleblowers should be protected against retaliation, a concept embodied in the provisions of the False Claims Act. In some cases, employees may sue their employers under the False Claims Act's qui tam provisions out of frustration because of the company's failure to act when a questionable, fraudulent, or abusive situation was brought to the attention of senior leaders.

Return to TOC

HHS Office of Inspector General

51

The Compliance Committee also should develop several independent reporting paths for an employee to directly report violations of Federal and State health care requirements, such as fraud, waste or abuse, and violations of entity policy, so that such reports cannot be diverted by supervisors or other personnel. The Compliance Committee should ensure that the entity does not deter individuals from coming forward with compliance concerns by, for example, requesting or requiring that personnel first bring such concerns to their manager or supervisor before contacting the compliance officer.

Tip **Frequent communications with the compliance officer from the same department or employees of the same supervisor may identify an area of concern to be investigated for possible compliance or human resources issues.**

The entity should have at least one reporting path independent of the business and operational functions that permits individuals to report concerns anonymously. **This could be through a hotline, a website, an email address, or a mailbox.** Options for anonymous reporting should be publicly posted in physical and virtual spaces frequently accessed by entity personnel.

Information about communicating compliance concerns, including the option to report anonymously, should be included in entity training about its compliance program.

The entity should always strive to maintain the confidentiality of the reporting employee's identity. But it also should explicitly communicate to any individual reporting a compliance concern that there may be a point where the individual's identity may become known or may have to be revealed. For example, in certain instances the entity may be required to inform governmental authorities.

All disclosures of compliance concerns, including potential violations of entity policies or Federal or State requirements, should be recorded in a log maintained by the compliance officer or their designee. All disclosures should be logged regardless of how they are made. whether made directly to the compliance officer or other compliance personnel, to another entity leader, or through the anonymous reporting mechanism, The entity's policies should require the compliance officer or their designee to record the disclosure promptly following receipt by the compliance officer or their designee.

Return to TOC

HHS Office of Inspector General

Some entities may have compliance departments, any member of whom may receive compliance concerns. Other entities may have facilities in multiple locations, each with their own facility compliance officer. Any of these would be considered designees.

The disclosure log should include pertinent information regarding each disclosure, such as the date received, the individual or department responsible for review, a description of the investigation's findings, any corrective actions taken, any policy or process changes made as a result of the investigation, the date resolved, and, if applicable, any resulting referral or disclosure to Federal or State authorities.

The compliance officer may take responsibility for reviewing some reported concerns, some reported concerns may be referred to other leaders or departments, for example, Human Resources, and some reports, such as those involving substantial legal violations, may be referred to counsel or law enforcement. The compliance officer should remain involved in all health care compliance investigations in which counsel takes the lead.

The compliance officer should regularly include information about concerns received and investigations conducted in their communications with the Compliance Committee and in their reports to the CEO and the board.

Return to TOC

HHS Office of Inspector General

E. Element 5—Enforcing Standards: Consequences and Incentives

For a compliance program to be effective, the organization should establish appropriate consequences for instances of noncompliance, as well as incentives for compliance. Consequences may involve remediation, sanctions, or both, depending on the facts. Incentives may be used to encourage compliance performance and innovation. Both incentives and consequences are important to enforcing compliance.

1. Consequences

Consequences, as used here, are the result of noncompliant actions. Consequences may be educational or remedial and non-punitive, they may be punitive sanctions, or they may involve both. Consequences may be appropriate where a responsible individual's failure to detect a violation is attributable to their ignorance, negligence, or reckless conduct. Intentional or reckless noncompliance should subject individuals to significant sanctions.

The organization should establish and publicize its procedures for identifying, investigating, and remediating (including re-training or discipline for the involved individuals) actions that do not comply with the entity's standards of conduct, policies and procedures, or Federal and State laws. The procedures should identify: the various consequences that may be imposed under specific circumstances involving noncompliance and the functions (e.g., manager, human resources) that will be involved in making decisions regarding appropriate consequences.

The entity should include in its guidance and compliance communications its commitment to take disciplinary action or impose other, remedial consequences on a fair and equitable basis. The compliance officer should monitor investigations and resulting discipline to ensure consistency. Managers and supervisors should be made aware that they have a responsibility to impose consequences for noncompliant behavior in an appropriate and consistent manner.

To deter noncompliant conduct, the consequences of noncompliance should be consistently applied and enforced. All levels of employees should be subject to the same consequences for the commission of similar offenses. The commitment to compliance applies to all personnel levels within an entity, including contractors and medical staff. OIG believes that corporate officers, managers, supervisors, health care professionals, and medical staff should be held accountable for failing to comply with, or for the foreseeable failure of their subordinates to adhere to, the applicable standards, laws, policies, and procedures.

Return to TOC

HHS Office of Inspector General

2. Incentives

Entities also should develop appropriate incentives to encourage participation in the entity's compliance program. The compliance officer, Compliance Committee, and other entity leaders should thoughtfully consider the compliance performance or activities they would like to incentivize, both across the entity and within specific departments or positions. Excellent compliance performance or significant contributions to the compliance program could be the basis for additional compensation, significant recognition, or other, smaller forms of encouragement.

Tip

Although an entity may not be able to publicly recognize an individual who raises a substantiated concern that results in the mitigation of harm or risk, the entity should find a way to recognize this in the performance reviews of individuals. This, of course, is not possible for people who wish to remain anonymous. Also, this does not apply to individuals who raise compliance or legal violations for which they themselves committed or were responsible.

Other behavior that entities may want to incentivize could include:

- the achievement of compliance goals that are specific to a department or a specific position description;
- achievements that reduce compliance risk (e.g., a team that develops a process that reduces compliance risk or enhances compliant outcomes, or an individual who suggests a method of attaining a strategic goal with less risk); or
- performance of compliance activities outside of the individual's job description (e.g., mentoring of colleagues in compliant performance or performing as a compliance representative within their department or team).

OIG encourages the compliance officer and the Compliance Committee to devote time, thought, and creativity to the compliance activities and contributions that the entity would like to incentivize.

The Compliance Committee and other entity leaders also should review whether the entity's other incentive plans can be achieved while operating in an ethical and compliant manner. The Compliance Committee should ask whether, for example, sales goals or admission goals may

Return to TOC

HHS Office of Inspector General

inadvertently encourage risky or noncompliant behavior such as offering health care practitioners things of value in exchange for ordering or prescribing an entity's products or referring patients to the entity's hospital or nursing home. The Compliance Committee also should examine whether setting certain performance goals may have unintended consequences, such as falsifying documents or covering up incidents that would detract from goal achievement.

Achievements in compliance should be treated commensurately with achievements in other areas valued by the entity. Through the thoughtful and deliberate use of incentives, an entity may reduce its compliance risk, enhance adherence to the entity's compliance program, and develop a positive association with the entity's compliance culture.

F. Element 6—Risk Assessment, Auditing, and Monitoring

Risk assessment, auditing, and monitoring each play a role in identifying and quantifying compliance risk. Although identifying and addressing risk have always been at the core of compliance programs, in recent years OIG, the compliance community, and other stakeholders have come to recognize and place increasing emphasis upon the importance of a formal compliance risk assessment process as part of the compliance program.

...in recent years OIG, the compliance community, and other stakeholders have come to recognize and place increasing emphasis upon the importance of a formal compliance risk assessment process as part of the compliance program.

1. Risk Assessment

Risk assessment is a process for identifying, analyzing, and responding to risk. A compliance risk assessment is a risk assessment process that looks at risk to the organization stemming from violations of law, regulations, or other legal requirements. For entities participating in or affected by government health care programs, a compliance risk assessment focuses on risks stemming from violations of government health care program requirements and other actions (or failures to act) that may adversely affect the entity's ability to comply with those requirements.

Return to TOC

HHS Office of Inspector General

56

Periodic compliance risk assessments should be a component of an entity's compliance program and should be conducted at least annually.

Entities that want to conduct compliance risk assessments more often should ensure that they dedicate the necessary time and resources for each compliance risk assessment they perform during the year.

A formal compliance risk assessment process should pull information about risks from a variety of external and internal sources, evaluate and prioritize them, and then decide which risks to address and how to address them. The Compliance Committee should be responsible for conducting and implementing the compliance risk assessment. The Compliance Committee may find it helpful to have compliance, audit, **quality**, and risk management functions coordinate to conduct a joint risk assessment to maximize the use of entity resources and reduce the number and potential redundancy of such assessments. With this information, the Compliance Committee can work with the compliance officer to prioritize resources and develop the compliance work plan, including audits and monitoring of identified risks based on priority. (Some entity functions, such as audit, may need to perform additional risk assessments to satisfy other requirements, such as fulfilling federal grant, contract, and other award obligations under 45 CFR § 75.303, for example.)

Although conducting formal risk assessments may be new to many compliance programs, risk assessments are an integral part of the fiscal internal control process and to enterprise risk management, and are required for recipients of federal awards. Compliance Committees should educate themselves on risk assessment methods when creating their own compliance risk assessment process. A standard resource for risk assessments is Enterprise Risk Management: Integrating with Strategy and Performance (2017), published by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission. The Society of Corporate Compliance and Ethics and the Health Care Compliance Association, with COSO, subsequently published Compliance Risk Management: Applying the COSO ERM Framework (2020), which contains information on conducting a compliance risk assessment. Another standard resource is The Green Book, published by the U.S. General Accountability Office, which contains a section on risk assessments. Playbook: Enterprise Risk Management for the U.S. Federal Government (Fall 2022 Update), published by the Chief Financial Officers Council and the Performance Improvement Council, provides useful risk-assessment tools in Appendices F and G. Numerous other guides and resources for conducting compliance risk assessments are available on the Internet.

Return to TOC

HHS Office of Inspector General

57

Entities should consider using data analytics, i.e., analyzing its data, to identify compliance risk areas. All entities, regardless of size, should have access to the data they generate, either directly or through a third party, such as a billing contractor. Data analytics efforts may range from simple to complex depending on an entity's volume of data as well as the entity's data analytics capabilities and resources.

All entities should be able to compare standard metrics of their health care operations internally to determine whether there are any outliers in any particular area of focus. Entities may use commonly available spreadsheet software to analyze their data. Other software programs that entities already use, such as billing software and electronic health records, may also have components that allow entities to analyze the data they contain. Larger entities or those with more capabilities or resources should run more sophisticated data analytics processes to assess any compliance risks presented by their operations. Analyzing data allows entities to identify possible risk areas by highlighting outliers or other data trends indicating potential noncompliance.

Between compliance risk assessments, the compliance officer should continue to scan for unidentified or new risks, by, for example, monitoring for legal and regulatory changes, enforcement actions and OIG work plan developments, and new entity acquisitions, strategies, or initiatives, and evaluating audits and investigation results. When the compliance officer or the Compliance Committee identifies a new risk, the risk should be assessed with the same methods used in the compliance risk assessment. Based on this information, the Compliance Committee can decide whether and how to address the newly identified risk.

2. Auditing and Monitoring

The Compliance Committee should include in the compliance work plan a schedule of audits to be conducted based on risks identified by the annual risk assessment. The Compliance Committee also should ensure that the compliance officer has the capacity to perform or oversee additional audits based on risks identified throughout the year, for example, as part of an investigation into an overpayment that uncovers a potential systemic issue. The audits may be conducted by internal or external auditors who have expertise in Federal and State health care statutes, regulations, and Federal health care program requirements.

Tip

Medicare requires, as a condition of payment, that items and services be medically reasonable and necessary. Therefore, entities should ensure that any claims reviews and audits include a review of the medical necessity of the item or service by an appropriately credentialed clinician. Entities that do not include clinical review of medical necessity in their claims audits may fail to identify important compliance concerns relating to medical necessity.

Depending on the entity's size, the entity may decide to have dedicated compliance auditors reporting to the compliance officer to conduct compliance audits.

The compliance work plan also should contain routine monitoring of ongoing risks, plus the capacity to monitor the effectiveness of controls and risk remediation. Examples of routine monitoring of known risks include:

- monthly screening of the LEIE and State Medicaid exclusion lists;
- regular screening of State licensure and certification databases; and
- annual review of the entity's policies and procedures.

Entities may identify other areas appropriate for routine monitoring based on their risk assessment and their interaction with the Federal health care programs, such as high-value billing codes, medical record documentation, medical necessity of admission, or business-need

Return to TOC

HHS Office of Inspector General

justifications for contracts with referral sources. Short-term monitoring is useful for determining the effectiveness of risk remediation.

Entities may wish, either periodically or during the annual risk assessment, to re-assess their ongoing monitoring program to determine whether monitoring is effective, still needed, or performed at the appropriate interval.

Entities also should periodically assess the compliance program's effectiveness. The review should include an assessment of how effective each element of the compliance program is. OIG has published a toolkit, Measuring Compliance Program Effectiveness, which may assist with this assessment. This toolkit provides a list of ideas, organized around the seven compliance program elements, from which health care organizations can select evaluative tools that will best serve their needs. It is intended to be a set of tools that any health care organization, regardless of size or health care industry segment, can use.

Tip **As OIG noted in its Introduction to Measuring Compliance Program Effectiveness, the toolkit is not intended to be a checklist to assess an entire compliance program. Using all the tools or many of them is impractical and not recommended.**

The board should direct the entity to perform the compliance program effectiveness review and have the reviewers report their findings and recommendations directly to the board. Depending on the entity's resources and recent compliance history (e.g., a large compliance failure or a series of events the compliance program did not identify and address as risks), the board may want to consider retaining an outside expert to conduct the review.

G. Element 7—Responding to Detected Offenses and Developing Corrective Action Initiatives

No matter how strong an entity's commitment to compliance or how effective the policies and procedures, training, and risk assessment, it is inevitable that a compliance officer will receive audit or monitoring results that raise concerns or receive a report through the disclosure program that requires investigating.

Tip **If, over time, a compliance officer does not receive this type of information, the compliance officer should consider conducting a compliance program effectiveness review.**

Return to TOC

HHS Office of Inspector General

60

An investigation could show that nothing improper occurred, it could reveal an overpayment that is owed, and it could uncover information indicating that misconduct has occurred, resulting in violations of applicable Federal or State law. Consequently, a compliance program should expect any outcome on this spectrum and plan accordingly through appropriate policies and other resources.

More specifically, compliance programs should include processes and resources to thoroughly investigate compliance concerns, take the steps necessary to remediate any legal or policy violations that are found, including reporting to any Government program agencies or law enforcement where appropriate, and analyze the root cause(s) of any identified impropriety to prevent a recurrence. How an entity responds when it finds a violation resulting in a substantial overpayment or serious misconduct sets apart those that have a strong compliance program from those with a compliance program that is more form than substance.

1. Investigations of Violations

Violations of an entity's compliance program, failures to comply with applicable Federal or State law, and other types of misconduct threaten an entity's status as a trustworthy organization capable of participating in Federal health care programs and the health care industry. Detected but uncorrected misconduct can seriously endanger the mission, reputation, and legal status of the entity. Consequently, it is important that the compliance officer act promptly to notify appropriate leaders and coordinate with entity counsel as needed upon receipt of reports or reasonable indications of suspected noncompliance to determine whether a material violation of applicable law has occurred.

Whether a material violation of applicable law exists must be determined on a case-by-case basis. The existence, or amount, of a monetary loss to a Federal health care program is not solely determinative of whether or not a violation has occurred. Allegations of noncompliant conduct should be investigated and the outcome of the investigation should determine whether, and what kind of, reporting to the Government is necessary. There may be material violations of applicable law where no monetary loss to a Federal health care program or Government entity has occurred; however, in these instances, corrective action and reporting (e.g., to CMS or a State Medicaid program) are still necessary to protect the integrity of the applicable program and its enrollees.

Return to TOC

HHS Office of Inspector General

61

Most internal investigations will require interviews and a review of relevant documents. Data review, email searches, and audits may also be required. The compliance officer or counsel should take appropriate steps to secure or prevent the destruction of documents or other evidence relevant to the investigation. Based on the potential scope and severity of the suspected violation and the necessary investigative tasks, entities should consider whether they need to engage external counsel, auditors, or health care experts to aid with the investigation. If counsel or the compliance officer believes the integrity of the investigation may be at stake because of the presence of employees under investigation, those subjects should be removed from their current work activity until the investigation is completed (unless an internal or Government-led undercover operation is in effect).

Regardless of the size or severity of the violation being investigated, a contemporaneous record of the investigation should be maintained, so that a record of the investigation can be compiled. The record should include:

- documentation of the alleged violation;
- a description of the investigative process;
- copies of interview notes and key document;
- a log of the witnesses interviewed and the documents reviewed;
- the results of the investigation; and
- any disciplinary action taken or corrective action implemented.

2. Reporting to the Government

This section endeavors to describe general guidelines related to reporting misconduct to the government. It does not address specific reporting requirements mandated by certain laws (e.g., HIPAA breach notification requirements; requirements related to reporting allegations of abuse and neglect in nursing facilities).

As a general matter, if credible evidence of misconduct from any source is discovered and, after a reasonable inquiry, the compliance officer or counsel has reason to believe that the misconduct may violate criminal, civil, or administrative law, then the entity should promptly (not more than 60 days after the determination that credible evidence of a violation exists) notify the appropriate Government authority of the misconduct.

Return to TOC

HHS Office of Inspector General

62

Depending on the nature of the violation and the Government program involved, appropriate Government authorities may include:

- the Criminal or Civil Divisions of DOJ;
- the United States Attorney's Office for the entity's district;
- OIG;
- CMS;
- the State Medicaid Fraud Control Units;
- the Defense Criminal Investigative Service;
- the Office of Inspector General for the Department of Veterans Affairs; and
- the Office of Personnel Management (which administers the Federal Employees Health Benefits Program).

Prompt reporting will demonstrate the entity's good faith and willingness to work with governmental authorities to correct and remedy the problem.

Some violations may be so serious that they warrant immediate notification to governmental authorities, prior to, or simultaneous with, commencing an internal investigation. This includes conduct that:

- is a clear violation of criminal law;
- has a significant adverse effect on either patient safety or the quality of care provided to patients (in addition to any other legal obligations regarding quality of care or abuse or neglect); or
- indicates evidence of a systemic failure to comply with applicable laws, an existing CIA, or other standards of conduct, regardless of the financial impact on Federal health care programs.

OIG believes in the importance of self-reporting. To facilitate this, OIG maintains voluntary self-disclosure programs for entities to use to report suspected fraud. OIG takes into consideration the entity's good-faith voluntary disclosure when resolving violations submitted through one of the programs. For more information about the OIG's voluntary self-disclosure programs and how entities can benefit from using them, please see our discussion in section VI.G.

Return to TOC

HHS Office of Inspector General

3. Implementing Corrective Action Initiatives

Once the entity has gathered sufficient credible information to determine the nature of the misconduct, it should take prompt corrective action, including:

- refunding of overpayments;
- enforcing disciplinary policies and procedures; and
- making any policy or procedure changes necessary to prevent a recurrence of the misconduct.

If the entity determines that the misconduct resulted in an overpayment, it should promptly repay the overpayment to affected government agencies. Federal law requires entities repay any overpayments received from Medicare or a State Medicaid program within 60 days after identification.[60] The entity should follow and enforce its policies and procedures against responsible individuals, including those in leadership or supervisory roles whose neglect or reckless disregard of their duties allowed the misconduct to occur unchecked or prevented the entity from identifying the misconduct earlier.

Throughout an investigation of any noncompliant conduct the compliance officer should be gathering information to aid them in determining the root causes of the conduct. The compliance officer should, of course, ensure that any ongoing noncompliant conduct is stopped and make any immediate changes necessary to ensure that it does not resume. But the compliance officer should also work with the appropriate individuals to determine the root cause of the conduct so that the entity can make the required changes to prevent a recurrence. The compliance officer should also determine whether the conduct exposed any compliance weaknesses that could place the entity at risk for other, unrelated misconduct. The Compliance Committee should ensure that the entity takes the necessary steps to prevent recurrence of the misconduct and to strengthen any identified areas of vulnerability.

[60] Section 1128J of the Act, 42 U.S.C. § 1320a-7k(d).

Return to TOC

SECTION IV
Compliance Program Adaptations for Small and Large Entities

Return to TOC

HHS Office of Inspector General

IV. Compliance Program Adaptations for Small and Large Entities

Compliance programs may be structured differently depending on the entity's size. Small entities and large organizations should think about how to right-size their compliance program to meet their entity's needs. Below, OIG provides guidance on how small entities can implement a compliance program that meets the seven elements even with limited resources. For large organizations, OIG discusses the role of the compliance officer, the Compliance Committee, and the board in developing and monitoring a compliance program capable of meeting the needs of a larger organization.

A. Compliance Programs for Small Entities

Small entities, such as individual and small-group physician practices, or other entities with a small number of employees, may face financial and staffing constraints that other entities do not. While still encompassing the seven elements discussed above, a small entity's compliance program should be structured so that the entity can gain the benefits and protection of a compliance program within the constraints under which the entity operates. OIG offers the following suggestions on how the seven elements can be successfully implemented at a small entity.

1. Compliance Contact

Small entities that cannot support a compliance officer on either a full-time or part-time basis should consider designating one person as the entity's compliance contact and have them be responsible for ensuring that the entity's compliance activities are completed. **This person should not have any responsibility for the performance or supervision of legal services to the entity and, whenever possible, should not be involved in the billing, coding, or submission of claims.** In the absence of a board, the compliance contact should report at least quarterly to the owner or CEO on the status of the entity's compliance activities. The owner or CEO is ultimately responsible for the entity's compliance with Federal health care program requirements.

Return to TOC

HHS Office of Inspector General

2. Policies, Procedures, and Training

A small entity should have policies, procedures, and training on how to perform duties and activities in compliance with government health care and other applicable legal requirements. It should also instruct its personnel on its compliance program.

Entities may be able to avail themselves of policy and procedure templates and training through their management company (if they use one), a consultant, or a professional organization. The internet may also be a source of policy and training material, although entities should review such material carefully for its content and quality and modify the material, as necessary, to reflect the specific business operations and compliance risks of the entity. Entities can supplement their own policies with information provided by applicable Federal agencies and contractors.

OIG maintains a series of Compliance Training Videos that entities may find helpful. Physician practices may also be able to obtain training through a hospital or other provider with which they are affiliated but should be mindful of potential Federal anti-kickback statute and physician self-referral implications that may arise from such arrangements.

Tip **OIG's guidance A Roadmap for New Physicians may be a helpful resource for experienced as well as new physicians. OIG also has a companion PowerPoint and speaker note set for trainers that are available on the same page.**

Small entities may educate their personnel on the entity's compliance program through a variety of means, including during an entity meeting, through email, on a website, or through postings in physical or virtual common areas. This information should be provided to new personnel when they join the entity and updates and reminders should be provided to personnel periodically.

Return to TOC

HHS Office of Inspector General

3. Open Lines of Communication

Although a formal disclosure program may not be necessary or appropriate for a small organization, a small entity should ensure that its personnel understand the entity's commitment to compliance and to nonretaliation.

Small entities should use user-friendly methods appropriate to their size and setting to facilitate communication about compliance concerns and potential issues. This may include an explicit "open door" policy for personnel to raise concerns with the compliance contact, the owner, or the CEO. This policy may be implemented in conjunction with less formal communication techniques, such as notices in physical or virtual common areas.

Even in the absence of a formal disclosure program, small entities should have policies in place that require good faith reporting of compliance issues or potential violations of law, outline a process for the investigation and resolution of reported issues or concerns, and prohibit retaliation for good faith reporting.

Other means that a small entity can use to facilitate meaningful and open communication include the following:

- the requirement that employees report conduct that a reasonable person would, in good faith, believe to be erroneous, improper, or fraudulent;
- the creation of a user-friendly process (such as an anonymous drop box) for effectively reporting erroneous, improper, or fraudulent conduct;
- a policy indicating that a failure to report erroneous, improper, or fraudulent conduct is a violation of the compliance program;
- the development of a simple and readily accessible procedure to process reports of erroneous, improper, or fraudulent conduct;
- if a billing company is used, communication to and from the billing company's compliance officer or compliance contact and other responsible staff to coordinate billing and compliance activities of the entity and the billing company, respectively;
- the utilization of a process that, if requested and to the extent possible, maintains the anonymity of the person reporting the concern; and

Return to TOC

HHS Office of Inspector General

- a policy indicating that there will be no retribution for reporting conduct that a reasonable person acting in good faith would have believed to be erroneous, improper, or fraudulent.

OIG recognizes that protecting anonymity may not be feasible for small entities. OIG believes, however, that all personnel seeking answers to questions or reporting potential instances of erroneous, improper, or fraudulent conduct should know to whom to turn for assistance in these matters and should be able to do so without fear of retribution.

While the entity may strive to maintain the anonymity of an employee's identity, it should also make clear that there may be a point at which the individual's identity may become known or may have to be revealed in certain instances. Small entities, particularly those for which anonymity is not possible, should post information about how to access the OIG Hotline in physical or virtual common areas.

4. Risk Assessment, Auditing, and Monitoring

Small entities should assess their compliance risks at least once a year.

Small entities that want to conduct compliance risk assessments more often should ensure that they dedicate the necessary time and resources for each compliance risk assessment they perform during the year. Small entities that receive federal awards should be sure to comply with requirements at 45 C.F.R. § 75.303.

Compliance risk assessments do not have to be complicated or resource intensive. Guidance and resources for conducting a compliance risk assessment are available on the Internet. One resource that may be of interest is Compliance Risk Management: Applying the COSO ERM Framework (2020), written by the Society of Corporate Compliance and Ethics and the Health Care Compliance Association. This resource discusses how to apply the enterprise risk management framework to compliance risk. It also has a section on conducting a compliance risk assessment. Small entities should review their own data to identify potential risks, such as claims denials, challenges to medical necessity, and patient safety data (e.g., fall rates, product-return rates, complaints). OIG regularly updates its Work Plan, which is also a good resource when attempting to identify potential risks. Small entities can also generate risk information by, for example, brainstorming during a staff meeting. After the small entity's risks are identified and analyzed, the entity can then decide how to address the high-priority issues, such as by conducting an audit, putting monitoring in place, or making process changes. Between

Return to TOC

HHS Office of Inspector General

compliance risk assessments, leaders should continue to watch for new or unidentified risks. If the small entity identifies a new risk, it should assess it and determine how to handle it.

Small entities should conduct at least an annual audit. The risk assessment can help the entity to determine what types of claims or other areas to select for the audit. Based on the audit results, the entity will be able to determine whether there are issues that it should address. Remediation could include:

- repayment of overpayments;
- changing of entity processes; and
- education of personnel.

Audit results may indicate that there could be potential systemic issues or they may identify potentially improper conduct. In that case, the entity should consider whether it needs to conduct an expanded audit or seek outside assistance to investigate and, if necessary, address and resolve the issue.

Risks that an entity becomes aware of outside of the annual risk assessment may require additional audits if the entity rates them as high priority.

Routine monitoring can be an effective and efficient method of managing known risks. This should include routine monitoring of the LEIE, applicable State Medicaid exclusion lists, and checks on practitioners' licensure and certification status.

Tip **An excluded employee or an employee with a lapsed license can have a significant impact on a small entity.**

Small entities should monitor communications they receive from the Federal health care programs and contractors so that they can make necessary policy changes to address new or revised program requirements.

Small entities can also develop a list of risk indicators relevant to their business or practice area for which they want to monitor, such as significant changes in number or type of claim rejections, high-level survey findings, illogical or atypical ordering patterns, and unusual changes in code utilization. When monitoring reveals one of these indicators, the entity should investigate to determine the cause of the indicator and then decide how to address it.

Return to TOC

HHS Office of Inspector General

5. Enforcing Standards

Small entities should ensure that they have enforcement and disciplinary mechanisms in place before violations of compliance policies, government health care requirements, or other applicable laws occur. The mechanisms should have sufficient flexibility to permit personnel to ask questions and disclose mistakes while also enforcing the entity's commitment to compliance. Entities might also want to communicate that the failure to report violations of compliance policies or legal requirements may lead to discipline. Entities may also want to consider implementing incentives for compliance performance and innovation.

For more information, see Element 5--Enforcing Standards: Consequences and Incentives

6. Responding to Detected Offenses and Developing Corrective Action Initiatives

When implementing a compliance program, small entities should anticipate that the program may uncover potential legal violations or other noncompliance.

Small entities should be prepared to designate someone, whether it is the compliance contact, an entity leader, or another designated employee, to determine whether a violation exists and the steps necessary to correct any problems. As appropriate, such steps could include:

- a corrective action plan;
- the return of overpayments;
- a report to the responsible government agency; or
- a disclosure to an appropriate law enforcement agency, such as a disclosure to the OIG.

A corrective action plan may include policy and process revisions, education of personnel, a revision to the entity's training plan, and consequences for offending individuals.

Return to TOC

HHS Office of Inspector General

71

B. Compliance Leadership for Large Entities

In prior board guidance, OIG wrote that health care board members should consider the size and complexity of their organizations in reviewing the scope and adequacy of the entity's compliance program. Whether a health care system in a large metropolitan area or a chain retail pharmacy or a manufacturer with locations and operations statewide or nationwide, large organizations will generally need significant compliance resources and expertise to develop and monitor a compliance program capable of addressing the breadth and complexity of compliance issues that a large organization faces. Boards of large health care organizations should thoughtfully evaluate the resources and expertise they will need at the compliance officer, Compliance Committee, and board level.

1. Compliance Officer

Large organizations are unlikely to implement and maintain a successful and effective compliance program with a single compliance officer. **A large organization will likely need a department of compliance personnel with a variety of skills and expertise to implement and monitor the organization's compliance program and address its manifold compliance needs.** A large organization should hire a knowledgeable and skilled compliance officer and leader as its chief compliance officer to oversee and direct the organization's compliance function and lead the compliance department.

Boards of large organizations should have input on the appointment, performance evaluation, and compensation of the chief compliance officer. They also should consider having the chief compliance officer report directly to them. Reporting to the board will give the chief compliance officer the stature and independence they need to lead a successful compliance program. In a large organization with many competing priorities, reporting directly to the board will send a strong message to the entire organization and its stakeholders about the board's commitment to compliance.

The chief compliance officer should organize the compliance department's staff to serve the organization most effectively. Depending on the structure and the nature of the organization, it may be useful to have one or more deputy compliance officers responsible for specific areas (e.g., compliance audits, investigations, training, policies) or components within the organization, regional compliance officers responsible for various geographic regions the organization serves, facility compliance officers or liaisons responsible for a specific facility or location, or some combination thereof.

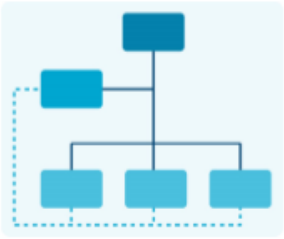
Return to TOC

The chief compliance officer should consider the varying skills that may be needed within the department, such as auditors, investigators, clinicians, and data experts, to operate effectively, and whether use of specialized consultants or part-time employees may be beneficial. If the large organization operates or controls a variety of providers and suppliers (for example, operating home health agencies and hospices and providing rehabilitation therapy services), the chief compliance officer should ensure that the compliance department has the compliance knowledge and expertise to address the compliance risks for each health care component the entity operates or controls.

The chief compliance officer and the board should periodically evaluate the compliance department to determine whether its current composition is effectively meeting the needs of the organization.

In a large organization with facilities or locations across a region or the country, it may be most effective to have dedicated compliance resources, such as a facility compliance officer (sometimes called a facility compliance liaison), at each facility or location.

Tip **To the extent possible, given the facility or location's staffing constraints, the facility compliance officer should not have responsibility for clinical, financial, legal, or operational duties.**



If the facility or location compliance officer responsibility is a part-time or secondary role that the individual assumed in addition to the position for which they were hired, the chief compliance officer should ensure that the facility or location compliance officer has a dotted-line reporting relationship to the chief compliance officer and is able to perform their compliance duties at the direction of the chief compliance officer (directly or indirectly through a deputy or regional compliance officer). This will ensure that all the compliance functions of the large organization are directed and overseen by the chief compliance officer. The chief compliance officer should also ensure that the facility or location compliance officer has the skills, knowledge, resources, and time to fulfill their compliance duties.

Return to TOC

HHS Office of Inspector General

2. Compliance Committee

The Compliance Committees of large organizations often have many members, representing the various operational components involved in the compliance program. Large-organization Compliance Committees may find it useful to create subcommittees to provide support to the chief compliance officer under the oversight of the Compliance Committee. Staffing subcommittees with a mix of Compliance Committee members and subject matter experts provides the Compliance Committee with additional expertise and ground-level experience while expanding involvement in the implementation and operation of the compliance program. Subcommittees may be responsible for policies and procedures, training and education, compliance audits, risk assessments, effective communication, and other areas pertinent to the organization. The Compliance Committee may also want to form temporary work groups to work on initiatives or other time-limited projects. Using subcommittees and work groups permits the Compliance Committee to substantively support the chief compliance officer while allowing more time at committee meetings for strategic and systemic compliance program matters.

3. Board Compliance Oversight

Boards of large organizations usually have separate board committees, such as a Board Audit Committee. Many boards assign the responsibility for compliance oversight to the Board Audit Committee. Boards should consider creating a separate Board Compliance Committee with a **charter** to oversee health care compliance. This permits each committee to focus on their area of responsibility. Separate committees can enable boards to ensure that each committee has members with knowledge and expertise in the Compliance Committee's area of responsibility. For example, compliance, government health care program requirements, and clinical or other expertise related to the organization's health care operations likely would be useful for the Board Compliance Committee, while members with audit, finance, and U.S. Securities and Exchange Commission expertise likely would be more useful for the Board Audit Committee. If the chief compliance officer reports to the board, the board may wish to delegate the responsibility for ongoing communication with the chief compliance officer to the Chair of the Board Compliance Committee or other board committee responsible for compliance.

Return to TOC

HHS Office of Inspector General

74

Some large organizations are owned or controlled by an international organization with headquarters located in another country. **Boards of large organizations operating in the United States but owned or controlled by international organizations should ensure that the parent board is provided with sufficient information about the applicable law, Federal health care program requirements, and the compliance risks presented by the operation of the U.S. organization.** Large organization boards with an international parent may wish to recommend that the parent board receive regular reports from and have the opportunity to engage in discussions with the chief compliance officer of the U.S. organization and counsel knowledgeable in the laws applicable to the U.S. organization (e.g., the False Claims Act, the Federal anti-kickback statute, and the PSL).

Return to TOC

HHS Office of Inspector General

SECTION V
Other Compliance Considerations

Return to TOC

HHS Office of Inspector General

V. Other Compliance Considerations

In this section, we offer some important compliance considerations related to several generally applicable risk areas.

Forthcoming ICPGs will address industry subsector-specific risk areas for different types of providers, suppliers, and other participants in health care industry subsectors or ancillary industry sectors relating to Federal health care programs. Our existing CPGs and supplemental CPGs will remain available for use as ongoing resources to help identify risk areas in particular industry segments as we develop the ICPGs.

We believe that this may further assist entities in developing policies and procedures, as well as implementing practices, to reduce or eliminate potential fraud and abuse risks in these areas. We will carefully consider timely updates and additions to this section based on general compliance concerns identified through OIG work, by the enforcement community, as well as feedback received from industry stakeholders through our email inbox at Compliance@oig.hhs.gov.

A. Quality and Patient Safety

Quality and patient safety are often treated as wholly separate and distinct from compliance, and the compliance program often does not contain quality and patient safety components. But quality and patient safety are integral to the work of HHS, CMS, FDA, and other agencies. And OIG and DOJ have long emphasized the importance of quality and patient safety. OIG and DOJ have investigated and settled cases based on the submission of false claims for care that is materially substandard, resulting in death or severe harm to patients. OIG has entered into CIAs focused on quality of care and patient safety. OIG has issued reports, toolkits, and board guidance on quality of care. Quality and patient safety are high priorities of HHS and DOJ.

Entities should incorporate quality and patient safety oversight into their compliance programs. Integrating quality and patient safety oversight into compliance processes can alert the entity of quality and patient safety concerns and enable the entity to mitigate risk of patient harm. Besides patient harm, quality and patient safety concerns, such as excessive services and medically unnecessary services, can lead to overpayments and may cause False Claims Act liability. The board should require regular reports from **senior leadership** responsible for

Return to TOC

77

quality and patient safety and from the compliance officer on oversight of quality and patient safety compliance. The board should receive regular reports on the system of internal quality controls, quality assurance monitoring, patient safety, and patient care.

The OIG guidance Corporate Responsibility and Health Care Quality: A Resource for Health Care Boards of Directors contains a helpful question-and-answer section on quality and compliance that entities and their boards may find useful in structuring board oversight. The board may also wish to utilize a quality dashboard to assist it in monitoring the entity's quality performance, including patient safety. OIG has provided guidance on dashboards for quality in Acute Care and Long-Term Care, which can provide useful information to boards in various health care sectors.

The Compliance Committee should include members responsible for quality assurance and patient safety. The Compliance Committee should receive regular reports from senior leadership on quality, patient safety, and, for provider entities and physician practices, adequacy of patient care. The Compliance Committee should establish and implement a program for performing quality audits and reviews. The program should:

- audit and review quality and patient safety incidents;
- conduct root-cause analyses;
- design or approve corrective action plans; and
- track the implementation and effectiveness of the plans.

Compliance Committees of entities directly furnishing patient care, particularly entities such as hospitals, long-term care facilities, and other entities providing residential care, should also assess staffing for nursing, therapy, and other clinical services to ensure that the entity has the appropriate quantity, quality, and composition of care providers.

The compliance officer should be responsible for implementing a compliance program that includes and addresses **quality** and patient safety compliance risks just as they do for any other compliance risk area integral to the entity's health care segment. To fulfill this responsibility, the compliance officer should:

Return to TOC

HHS Office of Inspector General

- develop productive working relationships with clinical and quality leadership, sharing information and work and advising on compliance matters;
- be informed about any internal quality audits and incident reviews; and
- have the resources to conduct the quality compliance audits discussed above, either individually or in collaboration with Internal Audit or outside resources.

When conducting risk assessments, Compliance Committees should ensure that medical necessity, patient safety, and other quality compliance issues are included in the risk universe. Medicare requires, as a condition of payment, that items and services be medically reasonable and necessary. Therefore, entities should ensure that any claims reviews and audits include a review of the medical necessity of the item or service by an appropriately credentialed clinician. Entities that do not include clinical review of medical necessity in their claims audits may fail to identify important compliance concerns relating to medical necessity.

B. New Entrants in the Health Care Industry

The health care sector is seeing an increasing number of new entrants, including technology companies (both established and start-up companies), new investors, and organizations providing non-traditional services in health care settings (such as social services, food delivery, and care coordination services). New entrants are often unfamiliar with the unique regulations and business constraints that apply in the health care industry, as well as the range of Federal and State government agencies that regulate health care and enforce fraud and abuse laws. Simply put, business practices that are common in other sectors create compliance risk in health care, including potential criminal, civil, and administrative liability. New entrants should take steps to ensure that they and any business partners possess a solid understanding of the Federal fraud and abuse laws, in addition to other applicable laws, and that they possess an understanding of the critical role an effective compliance program plays in preventing, detecting, and addressing potential violations. This GCPG is a practical tool that can assist new entrants in establishing and operating effective compliance programs for healthcare lines of business.

In addition, health care organizations are themselves entering new arenas. For example, providers are offering managed care plans and developing health care technology. While these organizations may be familiar with compliance risks applicable to their current business, they should also evaluate and familiarize themselves with new risk areas associated with new and different lines of health care business. Growing entities can consult OIG's existing compliance program guidance, advisory opinions, reports, and other compliance materials and forthcoming ICPGs to learn and keep updated about new risk areas.

Return to TOC

HHS Office of Inspector General

C. Financial Incentives: Ownership and Payment – Follow the Money

One of the best ways to identify fraud and abuse risks is to follow the money. In an increasingly complex health care ecosystem, understanding how funds flow through business arrangements and the varying incentives created by different types of funding structures is key to unearthing potential compliance issues, implementing effective monitoring, and identifying preventive strategies.

1. Ownership, including Private Equity and Others

The growing prominence of private equity and other forms of private investment in health care raises concerns about the impact of ownership incentives (e.g., return on investment) on the delivery of high quality, efficient health care. Health care entities, including their investors and governing bodies, should carefully scrutinize their operations and incentive structures to ensure compliance with the Federal fraud and abuse laws and that they are delivering high quality, safe care for patients. An understanding of the laws applicable to the health care industry and the role of an effective compliance program is particularly important for investors that provide management services or a significant amount of operational oversight for and control in a health care entity.

2. Payment Incentives

Compliance officers should be attuned to the varying risks associated with the payment methodologies through which health care entities are reimbursed for the items and services they provide. For example, when an insurer, including Federal health care programs, pays on a volume-sensitive or fee-for-service basis, there may be increased risks of overutilization, inappropriate patient steering, and use of more expensive items or services than needed. When an insurer pays on a capitated basis, heightened risks include stinting on care and discriminating against more costly patients. Payments that take into account quality of care or other performance measures may give rise to risk of gaming of data to qualify for performance-based payment. When payment incentives and associated risks are fully understood, compliance officers, including those at entities with private investment, are better positioned to design informed audit plans, conduct effective monitoring, detect problems early, and implement effective preventive strategies.

Return to TOC

HHS Office of Inspector General

D. Financial Arrangements Tracking

Entities involved in Federal health care program business may manage a significant volume of financial arrangements and transactional agreements, including those between referral sources and referral recipients, which can implicate the Federal anti-kickback statute and the PSL, among other Federal fraud and abuse laws. While legal counsel may be involved in the initial structuring and drafting of these agreements, ongoing monitoring of compliance with the terms and conditions set forth in the agreements remains equally important from a fraud and abuse perspective. Entities should consider what type of centralized arrangements tracking system to establish, depending on the size of their organization, to ensure that proper supporting documentation is maintained, regular legal reviews are conducted, and fair market value assessments are performed and updated routinely as appropriate. As applicable, tracking systems should also account for service and activity logs and use of lease space and equipment to ensure consistency with contract terms. The business need or rationale for arrangements should also be documented. An effective and robust arrangements tracking system—that is audited regularly—is a compliance measure that can be taken to prevent violations and mitigate potential liability under the Federal fraud and abuse laws.

Return to TOC

HHS Office of Inspector General

SECTION VI
OIG Resources and Processes

VI. OIG Resources and Processes

OIG has a Compliance Section on its website that includes numerous compliance and legal resources, such as our CPGs, Advisory Opinions, Special Fraud Alerts, Bulletins, and Other Guidance, Safe Harbor Regulations, Compliance Toolkits, Compliance Resources for Health Care Boards, Provider Compliance Training, A Roadmap for New Physicians, RAT-STATS - Statistical Software, Corporate Integrity Agreements (CIAs), and Self-Disclosure Information. We most recently added a more robust section on Frequently Asked Questions, with a new process for the health care community to submit questions, as discussed further below. In addition, under the Newsroom tab, we have short, educational videos covering a variety of substantive topics, Testimonies before Congress, as well as News Releases & Articles.

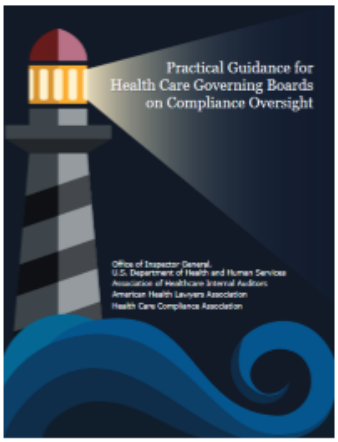
To stay up to date, we encourage you to subscribe to OIG's What's New Newsletter to receive email notifications when OIG has posted new information to our website, including reports, enforcement actions, and more. OIG also encourages you to subscribe to email notifications when the List of Excluded Individuals/Entities is updated. Lastly, OIG has various social media accounts that users can opt to follow to view OIG posts.

A. Compliance Toolkits; Compliance Resources for Health Care Boards; Provider Compliance Training; A Roadmap for New Physicians; and RAT-STATS Statistical Software

OIG has created several toolkits to provide the health care community with a structured approach to assess program integrity risks in telehealth, measure compliance program effectiveness, monitor adverse events, advise health care boards, and identify patients at risk of opioid misuse. The toolkit on measuring compliance program effectiveness is particularly important for all entities engaged in Federal health care program business to review. This guide lists measurement options applicable to a wide range of organizations with diverse size, operational complexity, industry segment focus, resources, and compliance programs. As discussed earlier in this document, we also created a webpage with compliance resources targeted specifically for health care boards that includes a document titled, Practical Guidance

Return to TOC

for Health Care Governing Boards on Compliance Oversight that covers topics on board roles and relationships, reporting to the board, identifying and auditing potential risk areas, and encouraging accountability and compliance. The Roadmap for New Physicians consists of educational materials and case examples to assist in teaching physicians about the Federal laws designed to protect the Federal health care programs and program beneficiaries from fraud, waste, and abuse. OIG offers additional training tools related to the Roadmap, including a brochure, companion PowerPoint presentation with speaker notes, as well as an audio narration.



OIG also makes available RAT-STATS statistical software that providers can download to assist in claims review. The package is the primary statistical tool for OIG's Office of Audit Services. Among other tasks, the software assists the user in selecting random samples and estimating improper payments. We have attempted to make RAT-STATS as user-friendly as possible, keeping in mind the program uses technical statistical terms.[61]

B. OIG Reports and Publications

OIG reports and publications are useful tools that can help identify risks to include in risk assessments, establish compliance priorities, and conduct targeted audits. Some of these materials include the OIG Work Plan; OIG Top Management Challenges; OIG Semiannual Reports to Congress; Health Care Fraud and Abuse Control Program Reports; Office of Audit Services Reports; and Office of Evaluation and Inspection Reports. These publications and reports can be consulted for both general risk trends as well as industry subsector-specific risks. In particular, the OIG Work Plan sets forth various projects, including OIG audits and evaluations, that are underway or planned to be addressed during the current fiscal year and beyond by OIG's Office of Audit Services and Office of Evaluation and Inspections. OIG assesses relative risks in HHS programs and operations to identify those areas most in need of attention and, accordingly, to set priorities for the sequence and proportion of resources to be allocated to conduct the reviews. The Work Plan is a web-based publication that describes the reviews OIG is planning and has underway, is updated monthly, and is searchable by topic.

Tip **The monthly update includes the addition of newly initiated Work Plan items, which can be found on the Recently Added Items page. Completed Work Plan items remain in the active Work Plan for**

[61] OIG does not provide technical support for RAT-STATS.

Return to TOC

HHS Office of Inspector General

one month, after which they are moved into the Archive. Recently completed reports can be found on OIG's What's New page.

C. Advisory Opinions; Special Fraud Alerts, Bulletins, and Other Guidance; and Safe Harbor Regulations

1. Advisory Opinions

OIG advisory opinions are the product of a statutorily mandated process that allows OIG to issue legal opinions to one or more requesting parties about the application of OIG's fraud and abuse authorities to the party's or parties' existing or proposed arrangement. A party that receives a favorable advisory opinion is prospectively protected from OIG administrative sanctions, so long as the arrangement at issue is conducted in accordance with the facts submitted to OIG through the advisory opinion process. While the goal of the advisory opinion process is to offer meaningful advice to the requestors of advisory opinions, the applicable statute and regulations make clear that advisory opinions are binding and may legally be relied upon only by the requestors of the applicable advisory opinion and the advisory opinion is only binding on the Secretary with respect to the requesting party.

We publish the redacted form of each issued advisory opinion on the OIG website for informational purposes, but again, no third parties are bound by or may legally rely upon these advisory opinions. OIG recognizes that stakeholders often look to published advisory opinions to understand OIG's views of particular arrangements and that advisory opinions may inform a party's review of a potential business arrangement, including identifying risks and potential application of safe harbors. It is important to be mindful that OIG relies on the certified facts and information submitted in connection with the applicable request and the advisory opinion that OIG ultimately renders is specific to the detailed facts certified by the applicable requestor. For more information about the advisory opinion process, including information regarding how to submit an advisory opinion request, please see OIG's overview of the advisory opinion process.

Return to TOC

HHS Office of Inspector General

2. Special Fraud Alerts, Bulletins, and Other Guidance; and Safe Harbor Regulations

OIG Special Fraud Alerts address specific trends of health care fraud of an industry-wide character. In developing Special Fraud Alerts, OIG relies on various sources, such as investigative trends identified from OI, DOJ, and state enforcement agencies as well as reports from OAS and OEI and industry feedback. We most recently issued special fraud alerts on telemedicine and speaker programs sponsored by pharmaceutical and medical device companies. OIG also issues Special Advisory Bulletins on various topics, such as Gifts and Other Inducements to Beneficiaries, Effect of Exclusion from Participation in Federal Health Care Programs, and Contractual Joint Ventures. Importantly, Other Guidance includes policy statements that help inform the public about changes to our procedural rules, enforcement priorities, and specific updates, such as what amounts are considered to be nominal value for the purposes of the Beneficiary Inducements CMP. Lastly, preamble text accompanying our safe harbor regulations can offer helpful insight into the development of the safe harbors and OIG's views on certain fraud and abuse risks and potential safeguards to protect against such risks, including responses received to comments submitted by health care stakeholders.

D. Frequently Asked Questions

OIG offers an FAQ process to provide informal feedback to the health care community on various topics. Beginning March 2023, OIG expanded the topics it considers for new FAQs submitted by the health care community. In particular, the agency reviews and considers: (1) general questions regarding the Federal anti-kickback statute and the Beneficiary Inducements CMP and OIG's administrative enforcement authorities in connection with these statutes; (2) inquiries regarding the general application of the Federal anti-kickback statute and Beneficiary Inducements CMP to a type of arrangement that may implicate these statutes; (3) questions regarding compliance considerations; and (4) inquiries regarding OIG's Health Care Fraud Self-Disclosure Protocol. OIG also reviews and considers general questions related to topics covered by FAQs existing as of March 2023, namely: (1) advisory opinions, (2) exclusions, and (3) its whistleblower protection coordinator function.

Return to TOC

The current list of topics addressed in FAQs include:

- General Questions Regarding Certain Fraud and Abuse Authorities;
- Application of Certain Fraud and Abuse Authorities to Certain Types of Arrangements;
- Compliance Considerations;
- Corporate Integrity Agreements;
- Exclusions;
- Contractor Self-Disclosures;
- Whistleblower Protection; and
- Advisory Opinions.

E. Corporate Integrity Agreements

OIG's Corporate Integrity Agreements and Integrity Agreements (CIA)[62] can serve as a resource when a health care entity reviews its compliance program's structure and operations. A CIA is a document that outlines the obligations to which an entity agrees as part of a civil or administrative settlement. An entity agrees to the CIA obligations in exchange for OIG's agreement that it will not seek to exclude the entity from participation in Medicare, Medicaid, or other Federal health care programs.

CIAs have common requirements that track the seven elements and require reviews to be conducted by independent review organizations (IROs). The subject matter of the IRO reviews required by a CIA can vary based on the underlying conduct that led to the settlement. For example, a case involving a Federal anti-kickback statute or PSL violation may lead to a CIA with a review of arrangements with referral sources while a case involving fraudulent billing would have a claims review. CIAs for pharmaceutical and device manufacturers typically have unique requirements to monitor their sales force activities, such as: a speaker monitoring program; direct field observations of sales personnel; and monitoring and review of other records relating to sales personnel's interactions with health care practitioners and health care institutions. Cases involving quality-of-care issues may result in a CIA with an independent monitor with clinical expertise appointed to examine the entity's delivery of care and evaluate

[62] An Integrity Agreement is a document that outlines the obligations to which an individual practitioner, small group practice, or small provider agrees as part of a civil or administrative settlement. IAs can serve as a valuable compliance resource for these entities, particularly when a small provider does not know where to begin with putting compliance measures scaled to their size in place.

Return to TOC

the provider's ability to prevent, detect, and respond to patient care problems. Other quality-of-care CIAs require the provider to retain a peer-review consultant to evaluate the provider's peer-review and medical-credentialing systems. We highlight these examples to illustrate how an entity that is not under a CIA could look to requirements for an entity in the same industry subsector that is under a CIA to glean ideas ranging from compliance program structure to external and internal audit plan designs.

F. Enforcement Action Summaries

When designing risk assessments and making determinations about compliance priorities, it can also help to consult information about enforcement actions posted on our website. When a matter is settled or otherwise resolved, OIG posts summaries and links to press releases, including those from our government partners, such as DOJ and State Attorney General Offices, with more information. Actions are categorized as follows on our website: Criminal and Civil, State Enforcement Agencies, CIA Reportable Events, CIA Stipulated Penalties and Material Breaches, Civil Monetary Penalties and Affirmative Exclusions, Self-Disclosure Settlements, and Grant Fraud Self-Disclosures. This information can also be useful to present to boards, organizational leaders, and employees and contractors when examples of problematic conduct can help illustrate the need for a particular compliance policy or action. They are also helpful to include as case examples in training materials.

G. OIG Self-Disclosure Information

OIG has several self-disclosure processes that can be used to report potential fraud in HHS programs.

Self-Disclosure Online Submissions

Health care providers, suppliers, or other individuals or entities subject to CMPs can use the Health Care Fraud Self-Disclosure Protocol to voluntarily disclose self-discovered evidence of potential fraud. Self-disclosure gives providers the opportunity to avoid the costs and disruptions associated with a Government-directed investigation and civil or administrative litigation.

Return to TOC

HHS Office of Inspector General

Tip **More detailed information about the OIG Health Care Fraud Self-Disclosure Protocol is available here.**

OIG's contractor self-disclosure program enables HHS contractors to self-disclose potential violations of the False Claims Act and various Federal criminal laws involving fraud, conflict of interest, bribery, or gratuity. Contractors are individuals, businesses, or other legal entities that are awarded Government contracts, or subcontracts, to provide services to HHS. The Contractor Self-Disclosure Program is available for those entities with a Federal Acquisition Regulation-based contract.

HHS grant recipients or subrecipients must disclose evidence of potential violations of Federal criminal law involving fraud, bribery, or gratuity violations, potentially affecting the Federal award. The governing regulation, 45 CFR § 75.113, mandates disclosures of criminal offenses that non-Federal entities must make with respect to HHS grants. Recipients of HHS awards may voluntarily disclose conduct creating CMP liability or any other conduct—such as conduct that might violate civil or administrative laws—that does not clearly fall within the scope of offenses described at 45 CFR § 75.113 through the HHS OIG Grant Self-Disclosure Program.

H. OIG Hotline

The OIG Hotline accepts tips and complaints from all sources about potential fraud, waste, abuse, and mismanagement in HHS programs.

Submit a Complaint

Every report we receive is important; however, not every submission results in an investigation. Due to the high volume of complaints OIG receives, it is not possible to contact every complainant. OIG recommends reviewing Before You Submit a Complaint to understand the type of complaints we do and do not investigate and the complaint process.

Return to TOC

HHS Office of Inspector General

SECTION VII
Conclusion

VII. Conclusion

This GCPG is intended to serve as a general compliance resource for the broad landscape of entities playing a role in health care delivery today. OIG recognizes that the health care industry in this country, which reaches millions of individuals and expends trillions of dollars annually, is constantly evolving. With this GCPG, we take the opportunity to both affirm and emphasize our longstanding and continuing commitment to support voluntary compliance efforts and to update and consolidate compliance tools and resources consistent with contemporary industry practices and current law. Because compliance is a dynamic process, OIG plans to update this GCPG as new developments occur and new resources become available. We also seek input from industry stakeholders who can submit feedback about general compliance considerations and risk areas to Compliance@oig.hhs.gov.

We also seek input from industry stakeholders who can submit feedback about general compliance considerations and risk areas to Compliance@oig.hhs.gov.

An effective compliance program is critical to meeting internal operational goals; decreasing errors; improving the quality of patient care and patient safety; and preventing, detecting, and addressing fraud, waste, and abuse. Consistent with OIG's mission, it is our goal that this GCPG and forthcoming ICPGs will be valuable tools in achieving these compliance successes.

Return to TOC

Definitions

Compliance Committee Charter

A statement of purpose, scope, roles and responsibilities, membership, meeting frequency, and other functions of the compliance committee.

Relevant Individuals

For the purposes of this GCPG, a "relevant individual" means a person whose responsibilities or activities are within the scope of the code, policy, or procedure. Relevant individuals could include employees, contractors, patients, customers, agency staff, medical staff, subcontractors, agents, or people in other roles, or a subset of the above. Each entity needs to determine for itself who their relevant individuals are.

Senior Leadership, Senior Leaders

For the purposes of the GCPG, "senior leadership" and "senior leaders" mean the group of leaders who report directly to the executive leading the entity, usually the CEO. Some entities refer to this group by other names, such as executive leadership.

Quality

For the purposes of this GCPG, "quality" means both quality in manufacturing and supplying drugs, devices, and other items, and quality of care in the provision of items and services.

Return to TOC

HHS Office of Inspector General

DOJ's 2020 Evaluation of Corporate Compliance Programs Guidance

U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

(Updated June 2020)

Introduction

The "Principles of Federal Prosecution of Business Organizations" in the Justice Manual describe specific factors that prosecutors should consider in conducting an investigation of a corporation, determining whether to bring charges, and negotiating plea or other agreements. JM 9-28.300. These factors include "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision" and the corporation's remedial efforts "to implement an adequate and effective corporate compliance program or to improve an existing one." JM 9-28.300 (citing JM 9-28.800 and JM 9-28.1000). Additionally, the United States Sentencing Guidelines advise that consideration be given to whether the corporation had in place at the time of the misconduct an effective compliance program for purposes of calculating the appropriate organizational criminal fine. *See* U.S.S.G. §§ 8B2.1, 8C2.5(f), and 8C2.8(11). Moreover, the memorandum entitled "Selection of Monitors in Criminal Division Matters" issued by Assistant Attorney General Brian Benczkowski (hereafter, the "Benczkowski Memo") instructs prosecutors to consider, at the time of the resolution, "whether the corporation has made significant investments in, and improvements to, its corporate compliance program and internal controls systems" and "whether remedial improvements to the compliance program and internal controls have been tested to demonstrate that they would prevent or detect similar misconduct in the future" to determine whether a monitor is appropriate.

This document is meant to assist prosecutors in making informed decisions as to whether, and to what extent, the corporation's compliance program was effective at the time of the offense, and is effective at the time of a charging decision or resolution, for purposes of determining the appropriate (1) form of any resolution or prosecution; (2) monetary penalty, if any; and (3) compliance obligations contained in any corporate criminal resolution (e.g., monitorship or reporting obligations).

Because a corporate compliance program must be evaluated in the specific context of a criminal investigation, the Criminal Division does not use any rigid formula to assess the effectiveness of corporate compliance programs. We recognize that each company's risk profile and solutions to reduce its risks warrant particularized evaluation. Accordingly, we make a reasonable, individualized determination in each case that considers various factors including, but not limited to, the company's size, industry, geographic footprint, regulatory landscape, and other factors, both internal and external to the company's operations, that might impact its compliance program. There are, however, common questions that we may ask in the course of making an individualized determination. As the Justice Manual notes, there are three "fundamental questions" a prosecutor should ask:

U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

(Updated June 2020)

1. "Is the corporation's compliance program well designed?"
2. "Is the program being applied earnestly and in good faith?" In other words, is the program adequately resourced and empowered to function effectively?
3. "Does the corporation's compliance program work" in practice?

See JM 9-28.800.

In answering each of these three "fundamental questions," prosecutors may evaluate the company's performance on various topics that the Criminal Division has frequently found relevant in evaluating a corporate compliance program both at the time of the offense and at the time of the charging decision and resolution.[1] The sample topics and questions below form neither a checklist nor a formula. In any particular case, the topics and questions set forth below may not all be relevant, and others may be more salient given the particular facts at issue and the circumstances of the company.[2] Even though we have organized the topics under these three fundamental questions, we recognize that some topics necessarily fall under more than one category.

I. Is the Corporation's Compliance Program Well Designed?

The "critical factors in evaluating any program are whether the program is adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees and whether corporate management is enforcing the program or is tacitly encouraging or pressuring employees to engage in misconduct." JM 9-28.800.

Accordingly, prosecutors should examine "the comprehensiveness of the compliance program," JM 9-28.800, ensuring that there is not only a clear message that misconduct is not tolerated, but also policies and procedures – from appropriate assignments of responsibility, to training programs, to systems of incentives and discipline – that ensure the compliance program is well-integrated into the company's operations and workforce.

A. Risk Assessment

The starting point for a prosecutor's evaluation of whether a company has a well-designed compliance program is to understand the company's business from a commercial perspective, how the company has identified, assessed, and defined its risk profile, and the degree to which the program devotes appropriate scrutiny and resources to the spectrum of risks. In short, prosecutors should endeavor to understand why the company has chosen to set up the compliance program the way that it has, and why and how the company's compliance program has evolved over time.

U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

(Updated June 2020)

Prosecutors should consider whether the program is appropriately "designed to detect the particular types of misconduct most likely to occur in a particular corporation's line of business" and "complex regulatory environment[]." JM 9-28.800.[3] For example, prosecutors should consider whether the company has analyzed and addressed the varying risks presented by, among other factors, the location of its operations, the industry sector, the competitiveness of the market, the regulatory landscape, potential clients and business partners, transactions with foreign governments, payments to foreign officials, use of third parties, gifts, travel, and entertainment expenses, and charitable and political donations.

Prosecutors should also consider "[t]he effectiveness of the company's risk assessment and the manner in which the company's compliance program has been tailored based on that risk assessment" and whether its criteria are "periodically updated." *See, e.g.*, JM 9-47-120(2)(c); U.S.S.G. § 8B2.1(c) ("the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement [of the compliance program] to reduce the risk of criminal conduct").

Prosecutors may credit the quality and effectiveness of a risk-based compliance program that devotes appropriate attention and resources to high-risk transactions, even if it fails to prevent an infraction. Prosecutors should therefore consider, as an indicator of risk-tailoring, "revisions to corporate compliance programs in light of lessons learned." JM 9-28.800.

- **Risk Management Process** – What methodology has the company used to identify, analyze, and address the particular risks it faces? What information or metrics has the company collected and used to help detect the type of misconduct in question? How have the information or metrics informed the company's compliance program?

- **Risk-Tailored Resource Allocation –** Does the company devote a disproportionate amount of time to policing low-risk areas instead of high-risk areas, such as questionable payments to third-party consultants, suspicious trading activity, or excessive discounts to resellers and distributors? Does the company give greater scrutiny, as warranted, to high-risk transactions (for instance, a large-dollar contract with a government agency in a high-risk country) than more modest and routine hospitality and entertainment?

- **Updates and Revisions** – Is the risk assessment current and subject to periodic review? Is the periodic review limited to a "snapshot" in time or based upon continuous access to operational data and information across functions? Has the periodic review led to updates in policies, procedures, and controls? Do these updates account for risks discovered through misconduct or other problems with the compliance program?

- **Lessons Learned** – Does the company have a process for tracking and incorporating into its periodic risk assessment lessons learned either from the company's own prior issues or from those of other companies operating in the same industry and/or geographical region?

B. Policies and Procedures

Any well-designed compliance program entails policies and procedures that give both content and effect to ethical norms and that address and aim to reduce risks identified by the company as part of its risk assessment process. As a threshold matter, prosecutors should examine whether the company has a code of conduct that sets forth, among other things, the company's commitment to full compliance with relevant Federal laws that is accessible and applicable to all company employees. As a corollary, prosecutors should also assess whether the company has established policies and procedures that incorporate the culture of compliance into its day-to-day operations.

- **Design** – What is the company's process for designing and implementing new policies and procedures and updating existing policies and procedures, and has that process changed over time? Who has been involved in the design of policies and procedures? Have business units been consulted prior to rolling them out?

- **Comprehensiveness** – What efforts has the company made to monitor and implement policies and procedures that reflect and deal with the spectrum of risks it faces, including changes to the legal and regulatory landscape?

- **Accessibility** – How has the company communicated its policies and procedures to all employees and relevant third parties? If the company has foreign subsidiaries, are there linguistic or other barriers to foreign employees' access? Have the policies and procedures been published in a searchable format for easy reference? Does the company track access to various policies and procedures to understand what policies are attracting more attention from relevant employees?

- **Responsibility for Operational Integration** – Who has been responsible for integrating policies and procedures? Have they been rolled out in a way that ensures employees' understanding of the policies? In what specific ways are compliance policies and procedures reinforced through the company's internal control systems?

- **Gatekeepers** – What, if any, guidance and training has been provided to key gatekeepers in the control processes (*e.g.*, those with approval authority or

certification responsibilities)? Do they know what misconduct to look for? Do they know when and how to escalate concerns?

C. Training and Communications

Another hallmark of a well-designed compliance program is appropriately tailored training and communications.

Prosecutors should assess the steps taken by the company to ensure that policies and procedures have been integrated into the organization, including through periodic training and certification for all directors, officers, relevant employees, and, where appropriate, agents and business partners. Prosecutors should also assess whether the company has relayed information in a manner tailored to the audience's size, sophistication, or subject matter expertise. Some companies, for instance, give employees practical advice or case studies to address real-life scenarios, and/or guidance on how to obtain ethics advice on a case-by-case basis as needs arise. Other companies have invested in shorter, more targeted training sessions to enable employees to timely identify and raise issues to appropriate compliance, internal audit, or other risk management functions. Prosecutors should also assess whether the training adequately covers prior compliance incidents and how the company measures the effectiveness of its training curriculum.

Prosecutors, in short, should examine whether the compliance program is being disseminated to, and understood by, employees in practice in order to decide whether the compliance program is "truly effective." JM 9-28.800.

- **Risk-Based Training** – What training have employees in relevant control functions received? Has the company provided tailored training for high-risk and control employees, including training that addresses risks in the area where the misconduct occurred? Have supervisory employees received different or supplementary training? What analysis has the company undertaken to determine who should be trained and on what subjects?

- **Form/Content/Effectiveness of Training** – Has the training been offered in the form and language appropriate for the audience? Is the training provided online or in-person (or both), and what is the company's rationale for its choice? Has the training addressed lessons learned from prior compliance incidents? Whether online or in-person, is there a process by which employees can ask questions arising out of the trainings? How has the company measured the effectiveness of the training? Have employees been tested on what they have learned? How has the company addressed

employees who fail all or a portion of the testing? Has the company evaluated the extent to which the training has an impact on employee behavior or operations?

- **Communications about Misconduct** – What has senior management done to let employees know the company's position concerning misconduct? What communications have there been generally when an employee is terminated or otherwise disciplined for failure to comply with the company's policies, procedures, and controls (*e.g.*, anonymized descriptions of the type of misconduct that leads to discipline)?

- **Availability of Guidance** – What resources have been available to employees to provide guidance relating to compliance policies? How has the company assessed whether its employees know when to seek advice and whether they would be willing to do so?

D. Confidential Reporting Structure and Investigation Process

Another hallmark of a well-designed compliance program is the existence of an efficient and trusted mechanism by which employees can anonymously or confidentially report allegations of a breach of the company's code of conduct, company policies, or suspected or actual misconduct. Prosecutors should assess whether the company's complaint-handling process includes proactive measures to create a workplace atmosphere without fear of retaliation, appropriate processes for the submission of complaints, and processes to protect whistleblowers. Prosecutors should also assess the company's processes for handling investigations of such complaints, including the routing of complaints to proper personnel, timely completion of thorough investigations, and appropriate follow-up and discipline.

Confidential reporting mechanisms are highly probative of whether a company has "established corporate governance mechanisms that can effectively detect and prevent misconduct." JM 9-28.800; *see also* U.S.S.G. § 8B2.1(b)(5)(C) (an effectively working compliance program will have in place, and have publicized, "a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation").

- **Effectiveness of the Reporting Mechanism** – Does the company have an anonymous reporting mechanism and, if not, why not? How is the reporting mechanism publicized to the company's employees and other third parties? Has it been used? Does the company take measures to test whether employees are aware of the hotline and feel comfortable using it? How has the company assessed the seriousness of the

allegations it received? Has the compliance function had full access to reporting and investigative information?

- **Properly Scoped Investigations by Qualified Personnel** – How does the company determine which complaints or red flags merit further investigation? How does the company ensure that investigations are properly scoped? What steps does the company take to ensure investigations are independent, objective, appropriately conducted, and properly documented? How does the company determine who should conduct an investigation, and who makes that determination?

- **Investigation Response** – Does the company apply timing metrics to ensure responsiveness? Does the company have a process for monitoring the outcome of investigations and ensuring accountability for the response to any findings or recommendations?

- **Resources and Tracking of Results** – Are the reporting and investigating mechanisms sufficiently funded? How has the company collected, tracked, analyzed, and used information from its reporting mechanisms? Does the company periodically analyze the reports or investigation findings for patterns of misconduct or other red flags for compliance weaknesses? Does the company periodically test the effectiveness of the hotline, for example by tracking a report from start to finish?

E. Third Party Management

A well-designed compliance program should apply risk-based due diligence to its third-party relationships. Although the need for, and degree of, appropriate due diligence may vary based on the size and nature of the company, transaction, and third party, prosecutors should assess the extent to which the company has an understanding of the qualifications and associations of third-party partners, including the agents, consultants, and distributors that are commonly used to conceal misconduct, such as the payment of bribes to foreign officials in international business transactions.

Prosecutors should also assess whether the company knows the business rationale for needing the third party in the transaction, and the risks posed by third-party partners, including the third-party partners' reputations and relationships, if any, with foreign officials. For example, a prosecutor should analyze whether the company has ensured that contract terms with third parties specifically describe the services to be performed, that the third party is actually performing the work, and that its compensation is commensurate with the work being provided in that industry and geographical region. Prosecutors should further assess whether the

company engaged in ongoing monitoring of the third-party relationships, be it through updated due diligence, training, audits, and/or annual compliance certifications by the third party.

In sum, a company's third-party management practices are a factor that prosecutors should assess to determine whether a compliance program is in fact able to "detect the particular types of misconduct most likely to occur in a particular corporation's line of business." JM 9-28.800.

- **Risk-Based and Integrated Processes** – How has the company's third-party management process corresponded to the nature and level of the enterprise risk identified by the company? How has this process been integrated into the relevant procurement and vendor management processes?

- **Appropriate Controls** – How does the company ensure there is an appropriate business rationale for the use of third parties? If third parties were involved in the underlying misconduct, what was the business rationale for using those third parties? What mechanisms exist to ensure that the contract terms specifically describe the services to be performed, that the payment terms are appropriate, that the described contractual work is performed, and that compensation is commensurate with the services rendered?

- **Management of Relationships** – How has the company considered and analyzed the compensation and incentive structures for third parties against compliance risks? How does the company monitor its third parties? Does the company have audit rights to analyze the books and accounts of third parties, and has the company exercised those rights in the past? How does the company train its third party relationship managers about compliance risks and how to manage them? How does the company incentivize compliance and ethical behavior by third parties? Does the company engage in risk management of third parties throughout the lifespan of the relationship, or primarily during the onboarding process?

- **Real Actions and Consequences** – Does the company track red flags that are identified from due diligence of third parties and how those red flags are addressed? Does the company keep track of third parties that do not pass the company's due diligence or that are terminated, and does the company take steps to ensure that those third parties are not hired or re-hired at a later date? If third parties were involved in the misconduct at issue in the investigation, were red flags identified from the due diligence or after hiring the third party, and how were they resolved? Has a similar third party been suspended, terminated, or audited as a result of compliance issues?

U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

(Updated June 2020)

F. Mergers and Acquisitions (M&A)

A well-designed compliance program should include comprehensive due diligence of any acquisition targets, as well as a process for timely and orderly integration of the acquired entity into existing compliance program structures and internal controls. Pre-M&A due diligence, where possible, enables the acquiring company to evaluate more accurately each target's value and negotiate for the costs of any corruption or misconduct to be borne by the target. Flawed or incomplete pre- or post-acquisition due diligence and integration can allow misconduct to continue at the target company, causing resulting harm to a business's profitability and reputation and risking civil and criminal liability.

The extent to which a company subjects its acquisition targets to appropriate scrutiny is indicative of whether its compliance program is, as implemented, able to effectively enforce its internal controls and remediate misconduct at all levels of the organization.

- **Due Diligence Process** – Was the company able to complete pre-acquisition due diligence and, if not, why not? Was the misconduct or the risk of misconduct identified during due diligence? Who conducted the risk review for the acquired/merged entities and how was it done? What is the M&A due diligence process generally?

- **Integration in the M&A Process** – How has the compliance function been integrated into the merger, acquisition, and integration process?

- **Process Connecting Due Diligence to Implementation** – What has been the company's process for tracking and remediating misconduct or misconduct risks identified during the due diligence process? What has been the company's process for implementing compliance policies and procedures, and conducting post-acquisition audits, at newly acquired entities?

II. Is the Corporation's Compliance Program Adequately Resourced and Empowered to Function Effectively?

Even a well-designed compliance program may be unsuccessful in practice if implementation is lax, under-resourced, or otherwise ineffective. Prosecutors are instructed to probe specifically whether a compliance program is a "paper program" or one "implemented, reviewed, and revised, as appropriate, in an effective manner." JM 9-28.800. In addition, prosecutors should determine "whether the corporation has provided for a staff sufficient to audit, document, analyze, and utilize the results of the corporation's compliance efforts." JM 9-28.800. Prosecutors should also determine "whether the corporation's employees are adequately informed about the compliance program and are convinced of the corporation's

commitment to it." JM 9-28.800; *see also* JM 9-47.120(2)(c) (criteria for an effective compliance program include "[t]he company's culture of compliance, including awareness among employees that any criminal conduct, including the conduct underlying the investigation, will not be tolerated").

A. Commitment by Senior and Middle Management

Beyond compliance structures, policies, and procedures, it is important for a company to create and foster a culture of ethics and compliance with the law at all levels of the company. The effectiveness of a compliance program requires a high-level commitment by company leadership to implement a culture of compliance from the middle and the top.

The company's top leaders – the board of directors and executives – set the tone for the rest of the company. Prosecutors should examine the extent to which senior management have clearly articulated the company's ethical standards, conveyed and disseminated them in clear and unambiguous terms, and demonstrated rigorous adherence by example. Prosecutors should also examine how middle management, in turn, have reinforced those standards and encouraged employees to abide by them. *See* U.S.S.G. § 8B2.1(b)(2)(A)-(C) (the company's "*governing authority* shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight" of it; "[*h*]*igh-level personnel* … shall ensure that the organization has an effective compliance and ethics program" (emphasis added)).

- **Conduct at the Top** – How have senior leaders, through their words and actions, encouraged or discouraged compliance, including the type of misconduct involved in the investigation? What concrete actions have they taken to demonstrate leadership in the company's compliance and remediation efforts? How have they modelled proper behavior to subordinates? Have managers tolerated greater compliance risks in pursuit of new business or greater revenues? Have managers encouraged employees to act unethically to achieve a business objective, or impeded compliance personnel from effectively implementing their duties?

- **Shared Commitment** – What actions have senior leaders and middle-management stakeholders (*e.g.*, business and operational managers, finance, procurement, legal, human resources) taken to demonstrate their commitment to compliance or compliance personnel, including their remediation efforts? Have they persisted in that commitment in the face of competing interests or business objectives?

- **Oversight** – What compliance expertise has been available on the board of directors? Have the board of directors and/or external auditors held executive or private sessions with the compliance and control functions? What types of information have

the board of directors and senior management examined in their exercise of oversight in the area in which the misconduct occurred?

B. Autonomy and Resources

Effective implementation also requires those charged with a compliance program's day-to-day oversight to act with adequate authority and stature. As a threshold matter, prosecutors should evaluate how the compliance program is structured. Additionally, prosecutors should address the sufficiency of the personnel and resources within the compliance function, in particular, whether those responsible for compliance have: (1) sufficient seniority within the organization; (2) sufficient resources, namely, staff to effectively undertake the requisite auditing, documentation, and analysis; and (3) sufficient autonomy from management, such as direct access to the board of directors or the board's audit committee. The sufficiency of each factor, however, will depend on the size, structure, and risk profile of the particular company. "A large organization generally shall devote more formal operations and greater resources . . . than shall a small organization." Commentary to U.S.S.G. § 8B2.1 note 2(C). By contrast, "a small organization may [rely on] less formality and fewer resources." *Id.* Regardless, if a compliance program is to be truly effective, compliance personnel must be empowered within the company.

Prosecutors should evaluate whether "internal audit functions [are] conducted at a level sufficient to ensure their independence and accuracy," as an indicator of whether compliance personnel are in fact empowered and positioned to "effectively detect and prevent misconduct." JM 9-28.800. Prosecutors should also evaluate "[t]he resources the company has dedicated to compliance," "[t]he quality and experience of the personnel involved in compliance, such that they can understand and identify the transactions and activities that pose a potential risk," and "[t]he authority and independence of the compliance function and the availability of compliance expertise to the board." JM 9-47.120(2)(c); *see also* JM 9-28.800 (instructing prosecutors to evaluate whether "the directors established an information and reporting system in the organization reasonably designed to provide management and directors with timely and accurate information sufficient to allow them to reach an informed decision regarding the organization's compliance with the law"); U.S.S.G. § 8B2.1(b)(2)(C) (those with "day-to-day operational responsibility" shall have "adequate resources, appropriate authority and direct access to the governing authority or an appropriate subgroup of the governing authority").

- **Structure** – Where within the company is the compliance function housed (e.g., within the legal department, under a business function, or as an independent function reporting to the CEO and/or board)? To whom does the compliance function report? Is the compliance function run by a designated chief compliance officer, or another executive within the company, and does that person have other roles within the company? Are compliance personnel dedicated to compliance responsibilities, or do

they have other, non-compliance responsibilities within the company? Why has the company chosen the compliance structure it has in place? What are the reasons for the structural choices the company has made?

- **Seniority and Stature** – How does the compliance function compare with other strategic functions in the company in terms of stature, compensation levels, rank/title, reporting line, resources, and access to key decision-makers? What has been the turnover rate for compliance and relevant control function personnel? What role has compliance played in the company's strategic and operational decisions? How has the company responded to specific instances where compliance raised concerns? Have there been transactions or deals that were stopped, modified, or further scrutinized as a result of compliance concerns?

- **Experience and Qualifications** – Do compliance and control personnel have the appropriate experience and qualifications for their roles and responsibilities? Has the level of experience and qualifications in these roles changed over time? How does the company invest in further training and development of the compliance and other control personnel? Who reviews the performance of the compliance function and what is the review process?

- **Funding and Resources** – Has there been sufficient staffing for compliance personnel to effectively audit, document, analyze, and act on the results of the compliance efforts? Has the company allocated sufficient funds for the same? Have there been times when requests for resources by compliance and control functions have been denied, and if so, on what grounds?

- **Data Resources and Access** – Do compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions? Do any impediments exist that limit access to relevant sources of data and, if so, what is the company doing to address the impediments?

- **Autonomy** – Do the compliance and relevant control functions have direct reporting lines to anyone on the board of directors and/or audit committee? How often do they meet with directors? Are members of the senior management present for these meetings? How does the company ensure the independence of the compliance and control personnel?

- **Outsourced Compliance Functions** – Has the company outsourced all or parts of its compliance functions to an external firm or consultant? If so, why, and who is responsible for overseeing or liaising with the external firm or consultant? What level of access does the external firm or consultant have to company information? How has the effectiveness of the outsourced process been assessed?

C. Incentives and Disciplinary Measures

Another hallmark of effective implementation of a compliance program is the establishment of incentives for compliance and disincentives for non-compliance. Prosecutors should assess whether the company has clear disciplinary procedures in place, enforces them consistently across the organization, and ensures that the procedures are commensurate with the violations. Prosecutors should also assess the extent to which the company's communications convey to its employees that unethical conduct will not be tolerated and will bring swift consequences, regardless of the position or title of the employee who engages in the conduct. *See* U.S.S.G. § 8B2.1(b)(5)(C) ("the organization's compliance program shall be promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct").

By way of example, some companies have found that publicizing disciplinary actions internally, where appropriate and possible, can have valuable deterrent effects. At the same time, some companies have also found that providing positive incentives – personnel promotions, rewards, and bonuses for improving and developing a compliance program or demonstrating ethical leadership – have driven compliance. Some companies have even made compliance a significant metric for management bonuses and/or have made working on compliance a means of career advancement.

- **Human Resources Process** – Who participates in making disciplinary decisions, including for the type of misconduct at issue? Is the same process followed for each instance of misconduct, and if not, why? Are the actual reasons for discipline communicated to employees? If not, why not? Are there legal or investigation-related reasons for restricting information, or have pre-textual reasons been provided to protect the company from whistleblowing or outside scrutiny?

- **Consistent Application** – Have disciplinary actions and incentives been fairly and consistently applied across the organization? Does the compliance function monitor its investigations and resulting discipline to ensure consistency? Are there similar instances of misconduct that were treated disparately, and if so, why?

- **Incentive System** – Has the company considered the implications of its incentives and rewards on compliance? How does the company incentivize compliance and ethical behavior? Have there been specific examples of actions taken (*e.g.*, promotions or awards denied) as a result of compliance and ethics considerations? Who determines the compensation, including bonuses, as well as discipline and promotion of compliance personnel?

III. Does the Corporation's Compliance Program Work in Practice?

The Principles of Federal Prosecution of Business Organizations require prosecutors to assess "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision." JM 9-28.300. Due to the backward-looking nature of the first inquiry, one of the most difficult questions prosecutors must answer in evaluating a compliance program following misconduct is whether the program was working effectively at the time of the offense, especially where the misconduct was not immediately detected.

In answering this question, it is important to note that the existence of misconduct does not, by itself, mean that a compliance program did not work or was ineffective at the time of the offense. *See* U.S.S.G. § 8B2.1(a) ("[t]he failure to prevent or detect the instant offense does not mean that the program is not generally effective in preventing and deterring misconduct"). Indeed, "[t]he Department recognizes that no compliance program can ever prevent all criminal activity by a corporation's employees." JM 9-28.800. Of course, if a compliance program did effectively identify misconduct, including allowing for timely remediation and self-reporting, a prosecutor should view the occurrence as a strong indicator that the compliance program was working effectively.

In assessing whether a company's compliance program was effective at the time of the misconduct, prosecutors should consider whether and how the misconduct was detected, what investigation resources were in place to investigate suspected misconduct, and the nature and thoroughness of the company's remedial efforts.

To determine whether a company's compliance program is working effectively at the time of a charging decision or resolution, prosecutors should consider whether the program evolved over time to address existing and changing compliance risks. Prosecutors should also consider whether the company undertook an adequate and honest root cause analysis to understand both what contributed to the misconduct and the degree of remediation needed to prevent similar events in the future.

For example, prosecutors should consider, among other factors, "whether the corporation has made significant investments in, and improvements to, its corporate compliance program and internal controls systems" and "whether remedial improvements to the compliance program and internal controls have been tested to demonstrate that they would prevent or detect similar misconduct in the future." Benczkowski Memo at 2 (observing that "[w]here a corporation's compliance program and controls are demonstrated to be effective and appropriately resourced at the time of resolution, a monitor will not likely be necessary").

A. Continuous Improvement, Periodic Testing, and Review

One hallmark of an effective compliance program is its capacity to improve and evolve. The actual implementation of controls in practice will necessarily reveal areas of risk and potential adjustment. A company's business changes over time, as do the environments in which it operates, the nature of its customers, the laws that govern its actions, and the applicable industry standards. Accordingly, prosecutors should consider whether the company has engaged in meaningful efforts to review its compliance program and ensure that it is not stale. Some companies survey employees to gauge the compliance culture and evaluate the strength of controls, and/or conduct periodic audits to ensure that controls are functioning well, though the nature and frequency of evaluations may depend on the company's size and complexity.

Prosecutors may reward efforts to promote improvement and sustainability. In evaluating whether a particular compliance program works in practice, prosecutors should consider "revisions to corporate compliance programs in light of lessons learned." JM 9-28.800; *see also* JM 9-47-120(2)(c) (looking to "[t]he auditing of the compliance program to assure its effectiveness"). Prosecutors should likewise look to whether a company has taken "reasonable steps" to "ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct," and "evaluate periodically the effectiveness of the organization's" program. U.S.S.G. § 8B2.1(b)(5). Proactive efforts like these may not only be rewarded in connection with the form of any resolution or prosecution (such as through remediation credit or a lower applicable fine range under the Sentencing Guidelines), but more importantly, may avert problems down the line.

- **Internal Audit** – What is the process for determining where and how frequently internal audit will undertake an audit, and what is the rationale behind that process? How are audits carried out? What types of audits would have identified issues relevant to the misconduct? Did those audits occur and what were the findings? What types of relevant audit findings and remediation progress have been reported to management and the board on a regular basis? How have management and the board followed up? How often does internal audit conduct assessments in high-risk areas?

- **Control Testing** – Has the company reviewed and audited its compliance program in the area relating to the misconduct? More generally, what testing of controls, collection and analysis of compliance data, and interviews of employees and third parties does the company undertake? How are the results reported and action items tracked?

- **Evolving Updates** – How often has the company updated its risk assessments and reviewed its compliance policies, procedures, and practices? Has the company undertaken a gap analysis to determine if particular areas of risk are not sufficiently addressed in its policies, controls, or training? What steps has the company taken to determine whether policies/procedures/practices make sense for particular business segments/subsidiaries? Does the company review and adapt its compliance program based upon lessons learned from its own misconduct and/or that of other companies facing similar risks?

- **Culture of Compliance** – How often and how does the company measure its culture of compliance? Does the company seek input from all levels of employees to determine whether they perceive senior and middle management's commitment to compliance? What steps has the company taken in response to its measurement of the compliance culture?

B. Investigation of Misconduct

Another hallmark of a compliance program that is working effectively is the existence of a well-functioning and appropriately funded mechanism for the timely and thorough investigations of any allegations or suspicions of misconduct by the company, its employees, or agents. An effective investigations structure will also have an established means of documenting the company's response, including any disciplinary or remediation measures taken.

- **Properly Scoped Investigation by Qualified Personnel** – How has the company ensured that the investigations have been properly scoped, and were independent, objective, appropriately conducted, and properly documented?

- **Response to Investigations** – Have the company's investigations been used to identify root causes, system vulnerabilities, and accountability lapses, including among supervisory managers and senior executives? What has been the process for responding to investigative findings? How high up in the company do investigative findings go?

U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

(Updated June 2020)

C. Analysis and Remediation of Any Underlying Misconduct

Finally, a hallmark of a compliance program that is working effectively in practice is the extent to which a company is able to conduct a thoughtful root cause analysis of misconduct and timely and appropriately remediate to address the root causes.

Prosecutors evaluating the effectiveness of a compliance program are instructed to reflect back on "the extent and pervasiveness of the criminal misconduct; the number and level of the corporate employees involved; the seriousness, duration, and frequency of the misconduct; and any remedial actions taken by the corporation, including, for example, disciplinary action against past violators uncovered by the prior compliance program, and revisions to corporate compliance programs in light of lessons learned." JM 9-28.800; *see also* JM 9-47.120(3)(c) ("to receive full credit for timely and appropriate remediation" under the FCPA Corporate Enforcement Policy, a company should demonstrate "a root cause analysis" and, where appropriate, "remediation to address the root causes").

Prosecutors should consider "any remedial actions taken by the corporation, including, for example, disciplinary action against past violators uncovered by the prior compliance program." JM 98-28.800; *see also* JM 9-47-120(2)(c) (looking to "[a]ppropriate discipline of employees, including those identified by the company as responsible for the misconduct, either through direct participation or failure in oversight, as well as those with supervisory authority over the area in which the criminal conduct occurred" and "any additional steps that demonstrate recognition of the seriousness of the misconduct, acceptance of responsibility for it, and the implementation of measures to reduce the risk of repetition of such misconduct, including measures to identify future risk").

- **Root Cause Analysis** – What is the company's root cause analysis of the misconduct at issue? Were any systemic issues identified? Who in the company was involved in making the analysis?

- **Prior Weaknesses** – What controls failed? If policies or procedures should have prohibited the misconduct, were they effectively implemented, and have functions that had ownership of these policies and procedures been held accountable?

- **Payment Systems** – How was the misconduct in question funded (*e.g.*, purchase orders, employee reimbursements, discounts, petty cash)? What processes could have prevented or detected improper access to these funds? Have those processes been improved?

- **Vendor Management** – If vendors were involved in the misconduct, what was the process for vendor selection and did the vendor undergo that process?

- **Prior Indications** – Were there prior opportunities to detect the misconduct in question, such as audit reports identifying relevant control failures or allegations, complaints, or investigations? What is the company's analysis of why such opportunities were missed?

- **Remediation** – What specific changes has the company made to reduce the risk that the same or similar issues will not occur in the future? What specific remediation has addressed the issues identified in the root cause and missed opportunity analysis?

- **Accountability** – What disciplinary actions did the company take in response to the misconduct and were they timely? Were managers held accountable for misconduct that occurred under their supervision? Did the company consider disciplinary actions for failures in supervision? What is the company's record (*e.g.*, number and types of disciplinary actions) on employee discipline relating to the types of conduct at issue? Has the company ever terminated or otherwise disciplined anyone (reduced or eliminated bonuses, issued a warning letter, etc.) for the type of misconduct at issue?

---

[1] Many of the topics also appear in the following resources:

- Justice Manual ("JM")
  - JM 9-28.000 Principles of Federal Prosecution of Business Organizations, Justice Manual ("JM"), *available at* https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations.
  - JM 9-47.120 FCPA Corporate Enforcement Policy, *available at* https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977#9-47.120.
- Chapter 8 – Sentencing of Organizations - United States Sentencing Guidelines ("U.S.S.G."), *available at* https://www.ussc.gov/guidelines/2018-guidelines-manual/2018-chapter-8#NaN.

- Memorandum entitled "Selection of Monitors in Criminal Division Matters," issued by Assistant Attorney General Brian Benczkowski on October 11, 2018, *available at* https://www.justice.gov/criminal-fraud/file/1100366/download.
- Criminal Division corporate resolution agreements, *available at* https://www.justice.gov/news (the Department of Justice's ("DOJ") Public Affairs website contains press releases for all Criminal Division corporate resolutions which contain links to charging documents and agreements).
- A Resource Guide to the U.S. Foreign Corrupt Practices Act ("FCPA Guide"), published in November 2012 by the DOJ and the Securities and Exchange Commission ("SEC"), *available at* https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf.
- Good Practice Guidance on Internal Controls, Ethics, and Compliance, adopted by the Organization for Economic Co-operation and Development ("OECD") Council on February 18, 2010, *available at* https://www.oecd.org/daf/anti-bribery/44884389.pdf.
- Anti-Corruption Ethics and Compliance Handbook for Business ("OECD Handbook"), published in 2013 by OECD, United Nations Office on Drugs and Crime, and the World Bank, *available at* https://www.oecd.org/corruption/Anti-CorruptionEthicsComplianceHandbook.pdf.
- Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations, published in July 2019 by DOJ's Antitrust Division, *available at* https://www.justice.gov/atr/page/file/1182001/download.
- A Framework for OFAC Compliance Commitments, published in May 2019 by the Department of the Treasury's Office of Foreign Assets Control ("OFAC"), *available at https://www.treasury.gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf.*

[2] Prosecutors should consider whether certain aspects of a compliance program may be impacted by foreign law. Where a company asserts that it has structured its compliance program in a particular way or has made a compliance decision based on requirements of foreign law, prosecutors should ask the company the basis for the company's conclusion about foreign law, and how the company has addressed the issue to maintain the integrity and effectiveness of its compliance program while still abiding by foreign law.

[3] As discussed in the Justice Manual, many companies operate in complex regulatory environments outside the normal experience of criminal prosecutors. JM 9-28.000. For example, financial institutions such as banks, subject to the Bank Secrecy Act statute and regulations,

require prosecutors to conduct specialized analyses of their compliance programs in the context of their anti-money laundering requirements. Consultation with the Money Laundering and Asset Recovery Section is recommended when reviewing AML compliance. *See* https://www.justice.gov/criminal-mlars. Prosecutors may also wish to review guidance published by relevant federal and state agencies. *See* Federal Financial Institutions Examination Council/Bank Secrecy Act/Anti-Money Laundering Examination Manual, *available at* https://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm).

DOJ's 2023 Evaluation of Corporate Compliance Programs Guidance

U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

(Updated March 2023)

Introduction

The "Principles of Federal Prosecution of Business Organizations" in the Justice Manual describe specific factors that prosecutors should consider in conducting an investigation of a corporation, determining whether to bring charges, and negotiating plea or other agreements. JM 9-28.300. These factors include "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision" and the corporation's remedial efforts "to implement an adequate and effective corporate compliance program or to improve an existing one." JM 9-28.300 (citing JM 9-28.800 and JM 9-28.1000). Additionally, the United States Sentencing Guidelines advise that consideration be given to whether the corporation had in place at the time of the misconduct an effective compliance program for purposes of calculating the appropriate organizational criminal fine. *See* U.S.S.G. §§ 8B2.1, 8C2.5(f), and 8C2.8(11). Moreover, Criminal Division policies on monitor selection instruct prosecutors to consider, at the time of the resolution, whether the corporation has made significant investments in, and improvements to, its corporate compliance program and internal controls systems and whether remedial improvements to the compliance program and internal controls have been tested to demonstrate that they would prevent or detect similar misconduct in the future to determine whether a monitor is appropriate.

This document is meant to assist prosecutors in making informed decisions as to whether, and to what extent, the corporation's compliance program was effective at the time of the offense, and is effective at the time of a charging decision or resolution, for purposes of determining the appropriate (1) form of any resolution or prosecution; (2) monetary penalty, if any; and (3) compliance obligations contained in any corporate criminal resolution (e.g., monitorship or reporting obligations).

Because a corporate compliance program must be evaluated in the specific context of a criminal investigation, the Criminal Division does not use any rigid formula to assess the effectiveness of corporate compliance programs. We recognize that each company's risk profile and solutions to reduce its risks warrant particularized evaluation. Accordingly, we make a reasonable, individualized determination in each case that considers various factors including, but not limited to, the company's size, industry, geographic footprint, regulatory landscape, and other factors, both internal and external to the company's operations, that might impact its compliance program. There are, however, common questions that we may ask in the course of making an individualized determination. As the Justice Manual notes, there are three "fundamental questions" a prosecutor should ask:

1. Is the corporation's compliance program well designed?
2. Is the program being applied earnestly and in good faith? In other words, is the program adequately resourced and empowered to function effectively?

3. Does the corporation's compliance program work in practice?

See JM 9-28.800.

In answering each of these three "fundamental questions," prosecutors may evaluate the company's performance on various topics that the Criminal Division has frequently found relevant in evaluating a corporate compliance program both at the time of the offense and at the time of the charging decision and resolution.[1] The sample topics and questions below form neither a checklist nor a formula. In any particular case, the topics and questions set forth below may not all be relevant, and others may be more salient given the particular facts at issue and the circumstances of the company.[2] Even though we have organized the topics under these three fundamental questions, we recognize that some topics necessarily fall under more than one category.

I. Is the Corporation's Compliance Program Well Designed?

The critical factors in evaluating any program are whether the program is adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees and whether corporate management is enforcing the program or is tacitly encouraging or permitting employees to engage in misconduct. JM 9-28.800.

Accordingly, prosecutors should examine the comprehensiveness of the compliance program, ensuring that there is not only a clear message that misconduct is not tolerated, but also policies and procedures – from appropriate assignments of responsibility, to training programs, to systems of incentives and discipline – that ensure the compliance program is well-integrated into the company's operations and workforce.

A. Risk Assessment

The starting point for a prosecutor's evaluation of whether a company has a well-designed compliance program is to understand the company's business from a commercial perspective, how the company has identified, assessed, and defined its risk profile, and the degree to which the program devotes appropriate scrutiny and resources to the spectrum of risks. In short, prosecutors should endeavor to understand why the company has chosen to set up the compliance program the way that it has, and why and how the company's compliance program has evolved over time.

Prosecutors should consider whether the program is appropriately "designed to detect [and prevent] the particular types of misconduct most likely to occur in a particular corporation's line of business" and "complex regulatory environment[]." JM 9-28.800.[3] For example, prosecutors should consider whether the company has analyzed and addressed the varying risks presented by, among other factors, the location of its operations, the industry sector, the competitiveness of the market, the regulatory landscape, potential clients and business partners, transactions with foreign governments, payments to foreign officials, use of third parties, gifts, travel, and entertainment expenses, and charitable and political donations.

Prosecutors should also consider "[t]he effectiveness of the company's risk assessment and the manner in which the company's compliance program has been tailored based on that risk assessment" and whether its criteria are "periodically updated." *See, e.g.*, JM 9-47-120(2)(c); U.S.S.G. § 8B2.1(c) ("the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement [of the compliance program] to reduce the risk of criminal conduct").

Prosecutors may credit the quality and effectiveness of a risk-based compliance program that devotes appropriate attention and resources to high-risk transactions, even if it fails to prevent an infraction. Prosecutors should therefore consider, as an indicator of risk-tailoring, "revisions to corporate compliance programs in light of lessons learned." JM 9-28.800.

- **Risk Management Process** – What methodology has the company used to identify, analyze, and address the particular risks it faces? What information or metrics has the company collected and used to help detect the type of misconduct in question? How have the information or metrics informed the company's compliance program?

- **Risk-Tailored Resource Allocation** – Does the company devote a disproportionate amount of time to policing low-risk areas instead of high-risk areas, such as questionable payments to third-party consultants, suspicious trading activity, or excessive discounts to resellers and distributors? Does the company give greater scrutiny, as warranted, to high-risk transactions (for instance, a large-dollar contract with a government agency in a high-risk country) than more modest and routine hospitality and entertainment?

- **Updates and Revisions** – Is the risk assessment current and subject to periodic review? Is the periodic review limited to a "snapshot" in time or based upon continuous access to operational data and information across functions? Has the periodic review led to updates in policies, procedures, and controls? Do these updates account for risks discovered through misconduct or other problems with the compliance program?

- **Lessons Learned** – Does the company have a process for tracking and incorporating into its periodic risk assessment lessons learned either from the company's own prior issues or from those of other companies operating in the same industry and/or geographical region?

B. Policies and Procedures

Any well-designed compliance program entails policies and procedures that give both content and effect to ethical norms and that address and aim to reduce risks identified by the company as part of its risk assessment process. As a threshold matter, prosecutors should examine whether the company has a code of conduct that sets forth, among other things, the company's commitment to full compliance with relevant Federal laws that is accessible and applicable to all

company employees. As a corollary, prosecutors should also assess whether the company has established policies and procedures that incorporate the culture of compliance into its day-to-day operations.

- **Design** – What is the company's process for designing and implementing new policies and procedures and updating existing policies and procedures, and has that process changed over time? Who has been involved in the design of policies and procedures? Have business units been consulted prior to rolling them out?

- **Comprehensiveness** – What efforts has the company made to monitor and implement policies and procedures that reflect and deal with the spectrum of risks it faces, including changes to the legal and regulatory landscape?

- **Accessibility** – How has the company communicated its policies and procedures to all employees and relevant third parties? If the company has foreign subsidiaries, are there linguistic or other barriers to foreign employees' access? Have the policies and procedures been published in a searchable format for easy reference? Does the company track access to various policies and procedures to understand what policies are attracting more attention from relevant employees?

- **Responsibility for Operational Integration** – Who has been responsible for integrating policies and procedures? Have they been rolled out in a way that ensures employees' understanding of the policies? In what specific ways are compliance policies and procedures reinforced through the company's internal control systems?

- **Gatekeepers** – What, if any, guidance and training has been provided to key gatekeepers in the control processes (*e.g.*, those with approval authority or certification responsibilities)? Do they know what misconduct to look for? Do they know when and how to escalate concerns?

C. Training and Communications

Another hallmark of a well-designed compliance program is appropriately tailored training and communications.

Prosecutors should assess the steps taken by the company to ensure that policies and procedures have been integrated into the organization, including through periodic training and certification for all directors, officers, relevant employees, and, where appropriate, agents and business partners. Prosecutors should also assess whether the company has relayed information in a manner tailored to the audience's size, sophistication, or subject matter expertise. Some companies, for instance, give employees practical advice or case studies to address real-life scenarios, and/or guidance on how to obtain ethics advice on a case-by-case basis as needs arise.

Other companies have invested in shorter, more targeted training sessions to enable employees to timely identify and raise issues to appropriate compliance, internal audit, or other risk management functions. Prosecutors should also assess whether the training adequately covers prior compliance incidents and how the company measures the effectiveness of its training curriculum.

Prosecutors, in short, should examine whether the compliance program is being disseminated to, and understood by, employees in practice in order to decide whether the compliance program is "truly effective." JM 9-28.800.

- **Risk-Based Training** – What training have employees in relevant control functions received? Has the company provided tailored training for high-risk and control employees, including training that addresses risks in the area where the misconduct occurred? Have supervisory employees received different or supplementary training? What analysis has the company undertaken to determine who should be trained and on what subjects?

- **Form/Content/Effectiveness of Training** – Has the training been offered in the form and language appropriate for the audience? Is the training provided online or in-person (or both), and what is the company's rationale for its choice? Has the training addressed lessons learned from prior compliance incidents? Whether online or in-person, is there a process by which employees can ask questions arising out of the trainings? How has the company measured the effectiveness of the training? Have employees been tested on what they have learned? How has the company addressed employees who fail all or a portion of the testing? Has the company evaluated the extent to which the training has an impact on employee behavior or operations?

- **Communications about Misconduct** – What has senior management done to let employees know the company's position concerning misconduct? What communications have there been generally when an employee is terminated or otherwise disciplined for failure to comply with the company's policies, procedures, and controls (*e.g.*, anonymized descriptions of the type of misconduct that leads to discipline)?

- **Availability of Guidance** – What resources have been available to employees to provide guidance relating to compliance policies? How has the company assessed whether its employees know when to seek advice and whether they would be willing to do so?

D. Confidential Reporting Structure and Investigation Process

Another hallmark of a well-designed compliance program is the existence of an efficient and trusted mechanism by which employees can anonymously or confidentially report allegations of a breach of the company's code of conduct, company policies, or suspected or actual

misconduct. Prosecutors should assess whether the company's complaint-handling process includes proactive measures to create a workplace atmosphere without fear of retaliation, appropriate processes for the submission of complaints, and processes to protect whistleblowers. Prosecutors should also assess the company's processes for handling investigations of such complaints, including the routing of complaints to proper personnel, timely completion of thorough investigations, and appropriate follow-up and discipline.

Confidential reporting mechanisms are highly probative of whether a company has established corporate governance mechanisms that can effectively detect and prevent misconduct. *See* U.S.S.G. § 8B2.1(b)(5)(C) (an effectively working compliance program will have in place, and have publicized, "a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation").

- **Effectiveness of the Reporting Mechanism** – Does the company have an anonymous reporting mechanism and, if not, why not? How is the reporting mechanism publicized to the company's employees and other third parties? Has it been used? Does the company take measures to test whether employees are aware of the hotline and feel comfortable using it? How has the company assessed the seriousness of the allegations it received? Has the compliance function had full access to reporting and investigative information?

- **Properly Scoped Investigations by Qualified Personnel** – How does the company determine which complaints or red flags merit further investigation? How does the company ensure that investigations are properly scoped? What steps does the company take to ensure investigations are independent, objective, appropriately conducted, and properly documented? How does the company determine who should conduct an investigation, and who makes that determination?

- **Investigation Response** – Does the company apply timing metrics to ensure responsiveness? Does the company have a process for monitoring the outcome of investigations and ensuring accountability for the response to any findings or recommendations?

- **Resources and Tracking of Results** – Are the reporting and investigating mechanisms sufficiently funded? How has the company collected, tracked, analyzed, and used information from its reporting mechanisms? Does the company periodically analyze the reports or investigation findings for patterns of misconduct or other red flags for compliance weaknesses? Does the company periodically test the effectiveness of the hotline, for example by tracking a report from start to finish?

U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

(Updated March 2023)

E. Third Party Management

A well-designed compliance program should apply risk-based due diligence to its third-party relationships. Although the need for, and degree of, appropriate due diligence may vary based on the size and nature of the company, transaction, and third party, prosecutors should assess the extent to which the company has an understanding of the qualifications and associations of third-party partners, including the agents, consultants, and distributors that are commonly used to conceal misconduct, such as the payment of bribes to foreign officials in international business transactions.

Prosecutors should also assess whether the company knows the business rationale for needing the third party in the transaction, and the risks posed by third-party partners, including the third-party partners' reputations and relationships, if any, with foreign officials. For example, a prosecutor should analyze whether the company has ensured that contract terms with third parties specifically describe the services to be performed, that the third party is actually performing the work, and that its compensation is commensurate with the work being provided in that industry and geographical region. Prosecutors should further assess whether the company engaged in ongoing monitoring of the third-party relationships, be it through updated due diligence, training, audits, and/or annual compliance certifications by the third party.

In sum, a company's third-party management practices are a factor that prosecutors should assess to determine whether a compliance program is in fact able to "detect [and prevent] the particular types of misconduct most likely to occur in a particular corporation's line of business." JM 9-28.800.

- **Risk-Based and Integrated Processes** – How has the company's third-party management process corresponded to the nature and level of the enterprise risk identified by the company? How has this process been integrated into the relevant procurement and vendor management processes?

- **Appropriate Controls** – How does the company ensure there is an appropriate business rationale for the use of third parties? If third parties were involved in the underlying misconduct, what was the business rationale for using those third parties? What mechanisms exist to ensure that the contract terms specifically describe the services to be performed, that the payment terms are appropriate, that the described contractual work is performed, and that compensation is commensurate with the services rendered?

- **Management of Relationships** – How has the company considered and analyzed the compensation and incentive structures for third parties against compliance risks? How does the company monitor its third parties? Does the company have audit rights to analyze the books and accounts of third parties, and has the company exercised those rights in the past? How does the company train its third-party relationship managers

about compliance risks and how to manage them? How does the company incentivize compliance and ethical behavior by third parties? Does the company engage in risk management of third parties throughout the lifespan of the relationship, or primarily during the onboarding process?

- **Real Actions and Consequences** – Does the company track red flags that are identified from due diligence of third parties and how those red flags are addressed? Does the company keep track of third parties that do not pass the company's due diligence or that are terminated, and does the company take steps to ensure that those third parties are not hired or re-hired at a later date? If third parties were involved in the misconduct at issue in the investigation, were red flags identified from the due diligence or after hiring the third party, and how were they resolved? Has a similar third party been suspended, terminated, or audited as a result of compliance issues?

F. Mergers and Acquisitions (M&A)

A well-designed compliance program should include comprehensive due diligence of any acquisition targets, as well as a process for timely and orderly integration of the acquired entity into existing compliance program structures and internal controls. Pre-M&A due diligence, where possible, enables the acquiring company to evaluate more accurately each target's value and negotiate for the costs of any corruption or misconduct to be borne by the target. Flawed or incomplete pre- or post-acquisition due diligence and integration can allow misconduct to continue at the target company, causing resulting harm to a business's profitability and reputation and risking civil and criminal liability.

The extent to which a company subjects its acquisition targets to appropriate scrutiny is indicative of whether its compliance program is, as implemented, able to effectively enforce its internal controls and remediate misconduct at all levels of the organization.

- **Due Diligence Process** – Was the company able to complete pre-acquisition due diligence and, if not, why not? Was the misconduct or the risk of misconduct identified during due diligence? Who conducted the risk review for the acquired/merged entities and how was it done? What is the M&A due diligence process generally?

- **Integration in the M&A Process** – How has the compliance function been integrated into the merger, acquisition, and integration process?

- **Process Connecting Due Diligence to Implementation** – What has been the company's process for tracking and remediating misconduct or misconduct risks identified during the due diligence process? What has been the company's process for implementing compliance policies and procedures, and conducting post-acquisition audits, at newly acquired entities?

U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

(Updated March 2023)

II. Is the Corporation's Compliance Program Adequately Resourced and Empowered to Function Effectively?

Even a well-designed compliance program may be unsuccessful in practice if implementation is lax, under-resourced, or otherwise ineffective. Prosecutors are instructed to probe specifically whether a compliance program is a "paper program" or one implemented, resourced, reviewed, and revised, as appropriate, in an effective manner. JM 9-28.800. In this regard, prosecutors should evaluate a corporation's method for assessing and addressing applicable risks and designing appropriate controls to manage these risks. In addition, prosecutors should determine whether the corporation has provided for a staff sufficient to audit, document, analyze, and utilize the results of the corporation's compliance efforts. Prosecutors should also determine "whether the corporation's employees are adequately informed about the compliance program and are convinced of the corporation's commitment to it." JM 9-28.800; *see also* JM 9-47.120(2)(c) (criteria for an effective compliance program include "[t]he company's culture of compliance, including awareness among employees that any criminal conduct, including the conduct underlying the investigation, will not be tolerated").

A. Commitment by Senior and Middle Management

Beyond compliance structures, policies, and procedures, it is important for a company to create and foster a culture of ethics and compliance with the law at all levels of the company. The effectiveness of a compliance program requires a high-level commitment by company leadership to implement a culture of compliance from the middle and the top.

The company's top leaders – the board of directors and executives – set the tone for the rest of the company. Prosecutors should examine the extent to which senior management have clearly articulated the company's ethical standards, conveyed and disseminated them in clear and unambiguous terms, and demonstrated rigorous adherence by example. Prosecutors should also examine how middle management, in turn, have reinforced those standards and encouraged employees to abide by them. *See* U.S.S.G. § 8B2.1(b)(2)(A)-(C) (the company's "*governing authority* shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight" of it; "[*h*]*igh-level personnel* … shall ensure that the organization has an effective compliance and ethics program" (emphasis added)).

- **Conduct at the Top** – How have senior leaders, through their words and actions, encouraged or discouraged compliance, including the type of misconduct involved in the investigation? What concrete actions have they taken to demonstrate leadership in the company's compliance and remediation efforts? How have they modelled proper behavior to subordinates? Have managers tolerated greater compliance risks in pursuit of new business or greater revenues? Have managers encouraged employees to act unethically to achieve a business objective, or impeded compliance personnel from effectively implementing their duties?

- **Shared Commitment** – What actions have senior leaders and middle-management stakeholders (*e.g.*, business and operational managers, finance, procurement, legal, human resources) taken to demonstrate their commitment to compliance or compliance personnel, including their remediation efforts? Have they persisted in that commitment in the face of competing interests or business objectives?

- **Oversight** – What compliance expertise has been available on the board of directors? Have the board of directors and/or external auditors held executive or private sessions with the compliance and control functions? What types of information have the board of directors and senior management examined in their exercise of oversight in the area in which the misconduct occurred?

B. Autonomy and Resources

Effective implementation also requires those charged with a compliance program's day-to-day oversight to act with adequate authority and stature. As a threshold matter, prosecutors should evaluate how the compliance program is structured. Additionally, prosecutors should address the sufficiency of the personnel and resources within the compliance function, in particular, whether those responsible for compliance have: (1) sufficient seniority within the organization; (2) sufficient resources, namely, staff to effectively undertake the requisite auditing, documentation, and analysis; and (3) sufficient autonomy from management, such as direct access to the board of directors or the board's audit committee. The sufficiency of each factor, however, will depend on the size, structure, and risk profile of the particular company. "A large organization generally shall devote more formal operations and greater resources . . . than shall a small organization." Commentary to U.S.S.G. § 8B2.1 note 2(C). By contrast, "a small organization may [rely on] less formality and fewer resources." *Id.* Regardless, if a compliance program is to be truly effective, compliance personnel must be empowered within the company.

Prosecutors should evaluate whether internal audit functions [are] conducted at a level sufficient to ensure their independence and accuracy, as an indicator of whether compliance personnel are in fact empowered and positioned to effectively detect and prevent misconduct. Prosecutors should also evaluate "[t]he resources the company has dedicated to compliance," "[t]he quality and experience of the personnel involved in compliance, such that they can understand and identify the transactions and activities that pose a potential risk," and "[t]he authority and independence of the compliance function and the availability of compliance expertise to the board." JM 9-47.120(2)(c); *see also* U.S.S.G. § 8B2.1(b)(2)(C) (those with "day-to-day operational responsibility" shall have "adequate resources, appropriate authority and direct access to the governing authority or an appropriate subgroup of the governing authority").

- **Structure** – Where within the company is the compliance function housed (e.g., within the legal department, under a business function, or as an independent function reporting to the CEO and/or board)? To whom does the compliance function report? Is the compliance function run by a designated chief compliance officer, or another executive

within the company, and does that person have other roles within the company? Are compliance personnel dedicated to compliance responsibilities, or do they have other, non-compliance responsibilities within the company? Why has the company chosen the compliance structure it has in place? What are the reasons for the structural choices the company has made?

- **Seniority and Stature** – How does the compliance function compare with other strategic functions in the company in terms of stature, compensation levels, rank/title, reporting line, resources, and access to key decision-makers? What has been the turnover rate for compliance and relevant control function personnel? What role has compliance played in the company's strategic and operational decisions? How has the company responded to specific instances where compliance raised concerns? Have there been transactions or deals that were stopped, modified, or further scrutinized as a result of compliance concerns?

- **Experience and Qualifications** – Do compliance and control personnel have the appropriate experience and qualifications for their roles and responsibilities? Has the level of experience and qualifications in these roles changed over time? How does the company invest in further training and development of the compliance and other control personnel? Who reviews the performance of the compliance function and what is the review process?

- **Funding and Resources** – Has there been sufficient staffing for compliance personnel to effectively audit, document, analyze, and act on the results of the compliance efforts? Has the company allocated sufficient funds for the same? Have there been times when requests for resources by compliance and control functions have been denied, and if so, on what grounds?

- **Data Resources and Access** – Do compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions? Do any impediments exist that limit access to relevant sources of data and, if so, what is the company doing to address the impediments?

- **Autonomy** – Do the compliance and relevant control functions have direct reporting lines to anyone on the board of directors and/or audit committee? How often do they meet with directors? Are members of the senior management present for these meetings? How does the company ensure the independence of the compliance and control personnel?

- **Outsourced Compliance Functions** – Has the company outsourced all or parts of its compliance functions to an external firm or consultant? If so, why, and who is responsible for overseeing or liaising with the external firm or consultant? What level of access does the external firm or consultant have to company information? How has the effectiveness of the outsourced process been assessed?

C. Compensation Structures and Consequence Management

Another hallmark of effective implementation of a compliance program is the establishment of incentives for compliance and disincentives for non-compliance. Prosecutors should assess whether the company has clear consequence management procedures (procedures to identify, investigate, discipline and remediate violations of law, regulation, or policy) in place, enforces them consistently across the organization, and ensures that the procedures are commensurate with the violations. Prosecutors should also assess the extent to which the company's communications convey to its employees that unethical conduct will not be tolerated and will bring swift consequences, regardless of the position or title of the employee who engages in the conduct. *See* U.S.S.G. § 8B2.1(b)(5)(C) ("the organization's compliance program shall be promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct").

By way of example, prosecutors may consider whether a company has publicized disciplinary actions internally, where appropriate and possible, which can have valuable deterrent effects. Prosecutors may also consider whether a company is tracking data relating to disciplinary actions to measure effectiveness of the investigation and consequence management functions. This can include monitoring the number of compliance-related allegations that are substantiated, the average (and outlier) times to complete a compliance investigation, and the effectiveness and consistency of disciplinary measures across the levels, geographies, units or departments of an organization.

The design and implementation of compensation schemes play an important role in fostering a compliance culture. Prosecutors may consider whether a company has incentivized compliance by designing compensation systems that defer or escrow certain compensation tied to conduct consistent with company values and policies. Some companies have also enforced contract provisions that permit the company to recoup previously awarded compensation if the recipient of such compensation is found to have engaged in or to be otherwise responsible for corporate wrongdoing. Finally, prosecutors may consider whether provisions for recoupment or reduction of compensation due to compliance violations or misconduct are maintained and enforced in accordance with company policy and applicable laws.

Compensation structures that clearly and effectively impose financial penalties for misconduct can deter risky behavior and foster a culture of compliance. At the same time,

providing positive incentives, such as promotions, rewards, and bonuses for improving and developing a compliance program or demonstrating ethical leadership, can drive compliance. Prosecutors should examine whether a company has made working on compliance a means of career advancement, offered opportunities for managers and employees to serve as a compliance "champion", or made compliance a significant metric for management bonuses. In evaluating whether the compensation and consequence management schemes are indicative of a positive compliance culture, prosecutors should consider the following factors:

- **Human Resources Process** – Who participates in making disciplinary decisions, including for the type of misconduct at issue? How transparent has the company been with the design and implementation of its disciplinary process? In circumstances where an executive has been exited from the company on account of a compliance violation, how transparent has the company been with employees about the terms of the separation? Are the actual reasons for discipline communicated to employees in all cases? If not, why not? Is the same process followed for each instance of misconduct, and if not, why? Has the company taken steps to restrict disclosure or access to information about the disciplinary process? Are there legal or investigation-related reasons for restricting information, or have pre-textual reasons been provided to protect the company from whistleblowing or outside scrutiny?

- **Disciplinary Measures** – What types of disciplinary actions are available to management when it seeks to enforce compliance policies? Does the company have policies or procedures in place to recoup compensation that would not have been achieved but for misconduct attributable directly or indirectly to the executive or employee? What policies and practices does the company have in place to put employees on notice that they will not benefit from any potential fruits of misconduct? With respect to the particular misconduct at issue, has the company made good faith efforts to follow its policies and practices in this respect?

- **Consistent Application** – Have disciplinary actions and incentives been fairly and consistently applied across the organization? Does the compliance function monitor its investigations and resulting discipline to ensure consistency? Are there similar instances of misconduct that were treated disparately, and if so, why? What metrics does the company apply to ensure consistency of disciplinary measures across all geographies, operating units, and levels of the organization?

- **Financial Incentive System** – Has the company considered the impact of its financial rewards and other incentives on compliance? Has the company evaluated whether commercial targets are achievable if the business operates within a compliant and ethical manner? What role does the compliance function have in designing and awarding financial incentives at senior levels of the organization? How does the company incentivize compliance and ethical behavior? What percentage of executive

compensation is structured to encourage enduring ethical business objectives? Are the terms of bonus and deferred compensation subject to cancellation or recoupment, to the extent available under applicable law, in the event that non-compliant or unethical behavior is exposed before or after the award was issued? Does the company have a policy for recouping compensation that has been paid, where there has been misconduct? Have there been specific examples of actions taken (*e.g.*, promotions or awards denied, compensation recouped or deferred compensation cancelled) as a result of compliance and ethics considerations?

- **Effectiveness** – How has the company ensured effective consequence management of compliance violations in practice? What insights can be taken from the management of a company's hotline that provide indicia of its compliance culture or its management of hotline reports? How do the substantiation rates compare for similar types of reported wrongdoing across the company (*i.e.* between two or more different states, countries, or departments) or compared to similarly situated companies, if known? Has the company undertaken a root cause analysis into areas where certain conduct is comparatively over or under reported? What is the average time for completion of investigations into hotline reports and how are investigations that are addressed inconsistently managed by the responsible department? What percentage of the compensation awarded to executives who have been found to have engaged in wrongdoing has been subject to cancellation or recoupment for ethical violations? Taking into account the relevant laws and local circumstances governing the relevant parts of a compensation scheme, how has the organization sought to enforce breaches of compliance or penalize ethical lapses? How much compensation has in fact been impacted (either positively or negatively) on account of compliance-related activities?

III. Does the Corporation's Compliance Program Work in Practice?

The Principles of Federal Prosecution of Business Organizations require prosecutors to assess "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision." JM 9-28.300. Due to the backward-looking nature of the first inquiry, one of the most difficult questions prosecutors must answer in evaluating a compliance program following misconduct is whether the program was working effectively at the time of the offense, especially where the misconduct was not immediately detected.

In answering this question, it is important to note that the existence of misconduct does not, by itself, mean that a compliance program did not work or was ineffective at the time of the offense. *See* U.S.S.G. § 8B2.1(a) ("[t]he failure to prevent or detect the instant offense does not mean that the program is not generally effective in preventing and deterring misconduct"). Indeed, "[t]he Department recognizes that no compliance program can prevent all criminal activity by a corporation's employees." JM 9-28.800. Of course, if a compliance program did effectively identify misconduct, including allowing for timely remediation and self-reporting, a prosecutor

should view the occurrence as a strong indicator that the compliance program was working effectively.

In assessing whether a company's compliance program was effective at the time of the misconduct, prosecutors should consider whether and how the misconduct was detected, what investigation resources were in place to investigate suspected misconduct, and the nature and thoroughness of the company's remedial efforts.

To determine whether a company's compliance program is working effectively at the time of a charging decision or resolution, prosecutors should consider whether the program evolved over time to address existing and changing compliance risks. Prosecutors should also consider whether the company undertook an adequate and honest root cause analysis to understand both what contributed to the misconduct and the degree of remediation needed to prevent similar events in the future.

A. Continuous Improvement, Periodic Testing, and Review

One hallmark of an effective compliance program is its capacity to improve and evolve. The actual implementation of controls in practice will necessarily reveal areas of risk and potential adjustment. A company's business changes over time, as do the environments in which it operates, the nature of its customers, the laws that govern its actions, and the applicable industry standards. Accordingly, prosecutors should consider whether the company has engaged in meaningful efforts to review its compliance program and ensure that it is not stale. Some companies survey employees to gauge the compliance culture and evaluate the strength of controls, and/or conduct periodic audits to ensure that controls are functioning well, though the nature and frequency of evaluations may depend on the company's size and complexity.

Prosecutors may reward efforts to promote improvement and sustainability. In evaluating whether a particular compliance program works in practice, prosecutors should consider "revisions to corporate compliance programs in light of lessons learned." JM 9-28.800; *see also* JM 9-47-120(2)(c) (looking to "[t]he auditing of the compliance program to assure its effectiveness"). Prosecutors should likewise look to whether a company has taken "reasonable steps" to "ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct," and "evaluate periodically the effectiveness of the organization's" program. U.S.S.G. § 8B2.1(b)(5). Proactive efforts like these may not only be rewarded in connection with the form of any resolution or prosecution (such as through remediation credit or a lower applicable fine range under the Sentencing Guidelines), but more importantly, may avert problems down the line.

- **Internal Audit** – What is the process for determining where and how frequently internal audit will undertake an audit, and what is the rationale behind that process? How are audits carried out? What types of audits would have identified issues relevant to the misconduct? Did those audits occur and what were the findings? What types of relevant audit findings and remediation progress have been reported to management

and the board on a regular basis? How have management and the board followed up? How often does internal audit conduct assessments in high-risk areas?

- **Control Testing** – Has the company reviewed and audited its compliance program in the area relating to the misconduct? More generally, what testing of controls, collection and analysis of compliance data, and interviews of employees and third parties does the company undertake? How are the results reported and action items tracked?

- **Evolving Updates** – How often has the company updated its risk assessments and reviewed its compliance policies, procedures, and practices? Has the company undertaken a gap analysis to determine if particular areas of risk are not sufficiently addressed in its policies, controls, or training? What steps has the company taken to determine whether policies/procedures/practices make sense for particular business segments/subsidiaries? Does the company review and adapt its compliance program based upon lessons learned from its own misconduct and/or that of other companies facing similar risks?

- **Culture of Compliance** – How often and how does the company measure its culture of compliance? How does the company's hiring and incentive structure reinforce its commitment to ethical culture? Does the company seek input from all levels of employees to determine whether they perceive senior and middle management's commitment to compliance? What steps has the company taken in response to its measurement of the compliance culture?

B. Investigation of Misconduct

Another hallmark of a compliance program that is working effectively is the existence of a well-functioning and appropriately funded mechanism for the timely and thorough investigations of any allegations or suspicions of misconduct by the company, its employees, or agents. An effective investigations structure will also have an established means of documenting the company's response, including any disciplinary or remediation measures taken.

- **Properly Scoped Investigation by Qualified Personnel** – How has the company ensured that the investigations have been properly scoped, and were independent, objective, appropriately conducted, and properly documented?

- **Response to Investigations** – Have the company's investigations been used to identify root causes, system vulnerabilities, and accountability lapses, including among supervisory managers and senior executives? What has been the process for responding to investigative findings? How high up in the company do investigative findings go?

- **Independence and Empowerment** – Is compensation for employees who are responsible for investigating and adjudicating misconduct structured in a way that ensures the compliance team is empowered to enforce the policies and ethical values of the company? Who determines the compensation, including bonuses, as well as discipline and promotion of compliance personnel or others within the organization that have a role in the disciplinary process generally?

Messaging applications have become ubiquitous in many markets and offer important platforms for companies to achieve growth and facilitate communication. In evaluating a corporation's policies and mechanisms for identifying, reporting, investigating, and remediating potential misconduct and violations of law, prosecutors should consider a corporation's policies and procedures governing the use of personal devices, communications platforms, and messaging applications, including ephemeral messaging applications. Policies governing such applications should be tailored to the corporation's risk profile and specific business needs and ensure that, as appropriate and to the greatest extent possible, business-related electronic data and communications are accessible and amenable to preservation by the company. Prosecutors should consider how the policies and procedures have been communicated to employees, and whether the corporation has enforced the policies and procedures on a regular and consistent basis in practice. In conducting this evaluation, prosecutors should consider the following factors:

- **Communication Channels** – What electronic communication channels do the company and its employees use, or allow to be used, to conduct business? How does that practice vary by jurisdiction and business function, and why? What mechanisms has the company put in place to manage and preserve information contained within each of the electronic communication channels? What preservation or deletion settings are available to each employee under each communication channel, and what do the company's policies require with respect to each? What is the rationale for the company's approach to determining which communication channels and settings are permitted?

- **Policy Environment** – What policies and procedures are in place to ensure that communications and other data is preserved from devices that are replaced? What are the relevant code of conduct, privacy, security, and employment laws or policies that govern the organization's ability to ensure security or monitor/access business-related communications? If the company has a "bring your own device" (BYOD) program, what are its policies governing preservation of and access to corporate data and communications stored on personal devices—including data contained within messaging platforms—and what is the rationale behind those policies? How have the company's data retention and business conduct policies been applied and enforced with respect to personal devices and messaging applications? Do the organization's policies permit the company to review business communications on BYOD and/or messaging applications? What exceptions or limitations to these policies have been permitted by

the organization? If the company has a policy regarding whether employees should transfer messages, data, and information from private phones or messaging applications onto company record-keeping systems in order to preserve and retain them, is it being followed in practice, and how is it enforced?

- **Risk Management** – What are the consequences for employees who refuse the company access to company communications? Has the company ever exercised these rights? Has the company disciplined employees who fail to comply with the policy or the requirement that they give the company access to these communications? Has the use of personal devices or messaging applications—including ephemeral messaging applications—impaired in any way the organization's compliance program or its ability to conduct internal investigations or respond to requests from prosecutors or civil enforcement or regulatory agencies? How does the organization manage security and exercise control over the communication channels used to conduct the organization's affairs? Is the organization's approach to permitting and managing communication channels, including BYOD and messaging applications, reasonable in the context of the company's business needs and risk profile?

C. Analysis and Remediation of Any Underlying Misconduct

Finally, a hallmark of a compliance program that is working effectively in practice is the extent to which a company is able to conduct a thoughtful root cause analysis of misconduct and timely and appropriately remediate to address the root causes.

Prosecutors evaluating the effectiveness of a compliance program are instructed to reflect back on "the extent and pervasiveness of the criminal misconduct; the number and level of the corporate employees involved; the seriousness, duration, and frequency of the misconduct; and any remedial actions taken by the corporation, including, for example, disciplinary action against past violators uncovered by the prior compliance program, and revisions to corporate compliance programs in light of lessons learned." JM 9-28.800; *see also* JM 9-47.120(3)(c) ("to receive full credit for timely and appropriate remediation" under the FCPA Corporate Enforcement Policy, a company should demonstrate "a root cause analysis" and, where appropriate, "remediation to address the root causes").

Prosecutors should consider "any remedial actions taken by the corporation, including, for example, disciplinary action against past violators uncovered by the prior compliance program." JM 98-28.800; *see also* JM 9-47-120(2)(c) (looking to "[a]ppropriate discipline of employees, including those identified by the company as responsible for the misconduct, either through direct participation or failure in oversight, as well as those with supervisory authority over the area in which the criminal conduct occurred" and "any additional steps that demonstrate recognition of the seriousness of the misconduct, acceptance of responsibility for it, and the implementation of measures to reduce the risk of repetition of such misconduct, including measures to identify future risk").

U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

(Updated March 2023)

- **Root Cause Analysis** – What is the company's root cause analysis of the misconduct at issue? Were any systemic issues identified? Who in the company was involved in making the analysis?

- **Prior Weaknesses** – What controls failed? If policies or procedures should have prohibited the misconduct, were they effectively implemented, and have functions that had ownership of these policies and procedures been held accountable?

- **Payment Systems** – How was the misconduct in question funded (*e.g.*, purchase orders, employee reimbursements, discounts, petty cash)? What processes could have prevented or detected improper access to these funds? Have those processes been improved?

- **Vendor Management** – If vendors were involved in the misconduct, what was the process for vendor selection and did the vendor undergo that process?

- **Prior Indications** – Were there prior opportunities to detect the misconduct in question, such as audit reports identifying relevant control failures or allegations, complaints, or investigations? What is the company's analysis of why such opportunities were missed?

- **Remediation** – What specific changes has the company made to reduce the risk that the same or similar issues will occur in the future? What specific remediation has addressed the issues identified in the root cause and missed opportunity analysis?

- **Accountability** – What disciplinary actions did the company take in response to the misconduct and were they timely? Were managers held accountable for misconduct that occurred under their supervision? Did the company consider disciplinary actions for failures in supervision? What is the company's record (*e.g.*, number and types of disciplinary actions) on employee discipline relating to the types of conduct at issue? Has the company ever terminated or otherwise disciplined anyone (reduced or eliminated bonuses, issued a warning letter, etc.) for the type of misconduct at issue? Did the company take any actions to recoup or reduce compensation for responsible employees to the extent practicable and available under applicable law?

---

[1] Many of the topics also appear in the following resources:

- Justice Manual ("JM")
    - JM 9-28.000 Principles of Federal Prosecution of Business Organizations, Justice Manual ("JM"), *available at* https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations.
    - JM 9-47.120 and the Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy, *available at* https://www.justice.gov/criminal-fraud/file/1562831/download.
- Chapter 8 – Sentencing of Organizations - United States Sentencing Guidelines ("U.S.S.G."), *available at* https://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2021/CHAPTER_8.pdf.
- Memorandum entitled "Selection of Monitors in Criminal Division Matters," issued by Assistant Attorney General Brian Benczkowski on October 11, 2018, *available at* https://www.justice.gov/criminal-fraud/file/1100366/download; updated Memorandum entitled "Selection of Monitors in Criminal Division Matters," issued by Assistant Attorney General Kenneth A. Polite, Jr., on March 1, 2023, *available at* https://www.justice.gov/criminal-fraud/file/1100366/download.
- Criminal Division corporate resolution agreements, *available at* https://www.justice.gov/news (the Department of Justice's ("DOJ") Public Affairs website contains press releases for all Criminal Division corporate resolutions which contain links to charging documents and agreements).
- A Resource Guide to the U.S. Foreign Corrupt Practices Act (2d ed.) ("FCPA Guide"), published in July 2020 by the DOJ and the Securities and Exchange Commission ("SEC"), *available at* https://www.justice.gov/criminal-fraud/file/1292051/download.
- Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions, amended by the Organization for Economic Co-operation and Development ("OECD") Council on November 25, 2021, *available at* https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0378.
- Anti-Corruption Ethics and Compliance Handbook for Business ("OECD Handbook"), published in 2013 by OECD, United Nations Office on Drugs and Crime, and the World Bank, *available at* https://www.oecd.org/corruption/Anti-CorruptionEthicsComplianceHandbook.pdf.
- Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations, published in July 2019 by DOJ's Antitrust Division, *available at* https://www.justice.gov/atr/page/file/1182001/download.

- A Framework for OFAC Compliance Commitments, published in May 2019 by the Department of the Treasury's Office of Foreign Assets Control ("OFAC"), *available at https://www.treasury.gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf.*

[2] Prosecutors should consider whether certain aspects of a compliance program may be impacted by foreign law. Where a company asserts that it has structured its compliance program in a particular way or has made a compliance decision based on requirements of foreign law, prosecutors should ask the company the basis for the company's conclusion about foreign law, and how the company has addressed the issue to maintain the integrity and effectiveness of its compliance program while still abiding by foreign law.

[3] As discussed in the Justice Manual, many companies operate in complex regulatory environments outside the normal experience of criminal prosecutors. JM 9-28.000. For example, financial institutions such as banks, subject to the Bank Secrecy Act statute and regulations, require prosecutors to conduct specialized analyses of their compliance programs in the context of their anti-money laundering requirements. Consultation with the Money Laundering and Asset Recovery Section is recommended when reviewing AML compliance. *See* https://www.justice.gov/criminal-mlars. Prosecutors may also wish to review guidance published by relevant federal and state agencies. *See* Federal Financial Institutions Examination Council/Bank Secrecy Act/Anti-Money Laundering Examination Manual, *available at* https://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm).

Redline Showing 2023 Changes to DOJ's 2020 Guidance

U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

(Updated ~~June 2020~~March 2023)

Introduction

The "Principles of Federal Prosecution of Business Organizations" in the Justice Manual describe specific factors that prosecutors should consider in conducting an investigation of a corporation, determining whether to bring charges, and negotiating plea or other agreements. JM 9-28.300. These factors include "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision" and the corporation's remedial efforts "to implement an adequate and effective corporate compliance program or to improve an existing one." JM 9-28.300 (citing JM 9-28.800 and JM ~~9-28.1000~~9-28.1000). Additionally, the United States Sentencing Guidelines advise that consideration be given to whether the corporation had in place at the time of the misconduct an effective compliance program for purposes of calculating the appropriate organizational criminal fine. *See* U.S.S.G. §§ 8B2.1, 8C2.5(f), and 8C2.8(11). Moreover, ~~the memorandum entitled "Selection of Monitors in~~ Criminal Division ~~Matters" issued by Assistant Attorney General Brian Benczkowski (hereafter, the "Benczkowski Memo") instructs~~policies on monitor selection instruct prosecutors to consider, at the time of the resolution, ~~"~~whether the corporation has made significant investments in, and improvements to, its corporate compliance program and internal controls systems~~"~~ and ~~"~~whether remedial improvements to the compliance program and internal controls have been tested to demonstrate that they would prevent or detect similar misconduct in the future~~"~~ to determine whether a monitor is appropriate.

This document is meant to assist prosecutors in making informed decisions as to whether, and to what extent, the corporation's compliance program was effective at the time of the offense, and is effective at the time of a charging decision or resolution, for purposes of determining the appropriate (1) form of any resolution or prosecution; (2) monetary penalty, if any; and (3) compliance obligations contained in any corporate criminal resolution (e.g., monitorship or reporting obligations).

Because a corporate compliance program must be evaluated in the specific context of a criminal investigation, the Criminal Division does not use any rigid formula to assess the effectiveness of corporate compliance programs. We recognize that each company's risk profile and solutions to reduce its risks warrant particularized evaluation. Accordingly, we make a reasonable, individualized determination in each case that considers various factors including, but not limited to, the company's size, industry, geographic footprint, regulatory landscape, and other factors, both internal and external to the company's operations, that might impact its compliance program. There are, however, common questions that we may ask in the course of making an individualized determination. As the Justice Manual notes, there are three "fundamental questions~~"~~" a prosecutor should ask:

~~U.S. Department of Justice~~
~~Criminal Division~~

~~Evaluation of Corporate Compliance Programs~~

~~(Updated June 2020)~~

1. ~~"~~Is the corporation's compliance program well designed?~~"~~

2. ~~"~~Is the program being applied earnestly and in good faith?~~"~~ In other words, is the program adequately resourced and empowered to function effectively?

1

U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

(Updated March 2023)

3. "Does the corporation's compliance program work" in practice? *See* JM 9-28.800.

In answering each of these three "fundamental questions," prosecutors may evaluate the company's performance on various topics that the Criminal Division has frequently found relevant in evaluating a corporate compliance program both at the time of the offense and at the time of the charging decision and resolution.[1] The sample topics and questions below form neither a checklist nor a formula. In any particular case, the topics and questions set forth below may not all be relevant, and others may be more salient given the particular facts at issue and the circumstances of the company.[2] Even though we have organized the topics under these three fundamental questions, we recognize that some topics necessarily fall under more than one category.

I. Is the Corporation's Compliance Program Well Designed?

The "critical factors in evaluating any program are whether the program is adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees and whether corporate management is enforcing the program or is tacitly encouraging or pressuringpermitting employees to engage in misconduct." JM 9-28.800.

Accordingly, prosecutors should examine "the comprehensiveness of the compliance program," JM 9-28.800, ensuring that there is not only a clear message that misconduct is not tolerated, but also policies and procedures – from appropriate assignments of responsibility, to training programs, to systems of incentives and discipline – that ensure the compliance program is well-integrated into the company's operations and workforce.

A. Risk Assessment

The starting point for a prosecutor's evaluation of whether a company has a well-designed compliance program is to understand the company's business from a commercial perspective, how the company has identified, assessed, and defined its risk profile, and the degree to which the program devotes appropriate scrutiny and resources to the spectrum of risks. In short, prosecutors should endeavor to understand why the company has chosen to set up the compliance program the way that it has, and why and how the company's compliance program has evolved over time.

~~U.S. Department of Justice~~
~~Criminal Division~~

~~Evaluation of Corporate Compliance Programs~~

~~(Updated June 2020)~~

Prosecutors should consider whether the program is appropriately "designed to detect [and prevent] the particular types of misconduct most likely to occur in a particular corporation's line of business" and "complex regulatory environment[]." JM 9-28.800.[3] For example, prosecutors should consider whether the company has analyzed and addressed the varying risks presented by, among other factors, the location of its operations, the industry sector, the competitiveness of the market, the regulatory landscape, potential clients and business partners, transactions with foreign governments, payments to foreign officials, use of third parties, gifts, travel, and entertainment expenses, and charitable and political donations.

U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

(Updated March 2023)

Prosecutors should also consider "[t]he effectiveness of the company's risk assessment and the manner in which the company's compliance program has been tailored based on that risk assessment" and whether its criteria are "periodically updated." *See, e.g.*, JM 9-47-120(2)(c); U.S.S.G. § 8B2.1(c) ("the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement [of the compliance program] to reduce the risk of criminal conduct").

Prosecutors may credit the quality and effectiveness of a risk-based compliance program that devotes appropriate attention and resources to high-risk transactions, even if it fails to prevent an infraction. Prosecutors should therefore consider, as an indicator of risk-tailoring, "revisions to corporate compliance programs in light of lessons learned." JM 9-28.800.

- **Risk Management Process** – What methodology has the company used to identify, analyze, and address the particular risks it faces? What information or metrics has the company collected and used to help detect the type of misconduct in question? How have the information or metrics informed the company's compliance program?

- **Risk-Tailored Resource Allocation** – Does the company devote a disproportionate amount of time to policing low-risk areas instead of high-risk areas, such as questionable payments to third-party consultants, suspicious trading activity, or excessive discounts to resellers and distributors? Does the company give greater scrutiny, as warranted, to high-risk transactions (for instance, a large-dollar contract with a government agency in a high-risk country) than more modest and routine hospitality and entertainment?

- **Updates and Revisions** – Is the risk assessment current and subject to periodic review? Is the periodic review limited to a "snapshot" in time or based upon continuous access to operational data and information across functions? Has the periodic review led to updates in policies, procedures, and controls? Do these updates account for risks discovered through misconduct or other problems with the compliance program?

- **Lessons Learned** – Does the company have a process for tracking and incorporating into its periodic risk assessment lessons learned either from the company's own prior issues or from those of other companies operating in the same industry and/or geographical region?

B. Policies and Procedures

Any well-designed compliance program entails policies and procedures that give both content and effect to ethical norms and that address and aim to reduce risks identified by the company as part of its risk assessment process. As a threshold matter, prosecutors should examine whether the company has a code of conduct that sets forth, among other things, the company's commitment to full compliance with relevant Federal laws that is accessible and applicable to all

company employees. As a corollary, prosecutors should also assess whether the company has established policies and procedures that incorporate the culture of compliance into its day-to-day operations.

- **Design** – What is the company's process for designing and implementing new policies and procedures and updating existing policies and procedures, and has that process changed over time? Who has been involved in the design of policies and procedures? Have business units been consulted prior to rolling them out?

- **Comprehensiveness** – What efforts has the company made to monitor and implement policies and procedures that reflect and deal with the spectrum of risks it faces, including changes to the legal and regulatory landscape?

- **Accessibility** – How has the company communicated its policies and procedures to all employees and relevant third parties? If the company has foreign subsidiaries, are there linguistic or other barriers to foreign employees' access? Have the policies and procedures been published in a searchable format for easy reference? Does the company track access to various policies and procedures to understand what policies are attracting more attention from relevant employees?

- **Responsibility for Operational Integration** – Who has been responsible for integrating policies and procedures? Have they been rolled out in a way that ensures employees' understanding of the policies? In what specific ways are compliance policies and procedures reinforced through the company's internal control systems?

- **Gatekeepers** – What, if any, guidance and training has been provided to key gatekeepers in the control processes (*e.g.*, those with approval authority or

certification responsibilities)? Do they know what misconduct to look for? Do they know when and how to escalate concerns?

C. Training and Communications

Another hallmark of a well-designed compliance program is appropriately tailored training and communications.

Prosecutors should assess the steps taken by the company to ensure that policies and procedures have been integrated into the organization, including through periodic training and certification for all directors, officers, relevant employees, and, where appropriate, agents and business partners. Prosecutors should also assess whether the company has relayed information in a manner tailored to the audience's size, sophistication, or subject matter expertise. Some companies, for instance, give employees practical advice or case studies to address real-life scenarios, and/or guidance on how to obtain ethics advice on a case-by-case basis as needs arise.

Other companies have invested in shorter, more targeted training sessions to enable employees to timely identify and raise issues to appropriate compliance, internal audit, or other risk management functions. Prosecutors should also assess whether the training adequately covers prior compliance incidents and how the company measures the effectiveness of its training curriculum.

Prosecutors, in short, should examine whether the compliance program is being disseminated to, and understood by, employees in practice in order to decide whether the compliance program is "truly effective." JM 9-28.800.

- **Risk-Based Training** – What training have employees in relevant control functions received? Has the company provided tailored training for high-risk and control employees, including training that addresses risks in the area where the misconduct occurred? Have supervisory employees received different or supplementary training? What analysis has the company undertaken to determine who should be trained and on what subjects?

- **Form/Content/Effectiveness of Training** – Has the training been offered in the form and language appropriate for the audience? Is the training provided online or in-person (or both), and what is the company's rationale for its choice? Has the training addressed lessons learned from prior compliance incidents? Whether online or in-person, is there a process by which employees can ask questions arising out of the trainings? How has the company measured the effectiveness of the training? Have employees been tested on what they have learned? How has the company addressed

employees who fail all or a portion of the testing? Has the company evaluated the extent to which the training has an impact on employee behavior or operations?

- **Communications about Misconduct** – What has senior management done to let employees know the company's position concerning misconduct? What communications have there been generally when an employee is terminated or otherwise disciplined for failure to comply with the company's policies, procedures, and controls (*e.g.*, anonymized descriptions of the type of misconduct that leads to discipline)?

- **Availability of Guidance** – What resources have been available to employees to provide guidance relating to compliance policies? How has the company assessed whether its employees know when to seek advice and whether they would be willing to do so?

D. Confidential Reporting Structure and Investigation Process

Another hallmark of a well-designed compliance program is the existence of an efficient and trusted mechanism by which employees can anonymously or confidentially report allegations of a breach of the company's code of conduct, company policies, or suspected or actual

misconduct. Prosecutors should assess whether the company's complaint-handling process includes proactive measures to create a workplace atmosphere without fear of retaliation, appropriate processes for the submission of complaints, and processes to protect whistleblowers. Prosecutors should also assess the company's processes for handling investigations of such complaints, including the routing of complaints to proper personnel, timely completion of thorough investigations, and appropriate follow-up and discipline.

Confidential reporting mechanisms are highly probative of whether a company has "established corporate governance mechanisms that can effectively detect and prevent misconduct." ~~JM 9-28.800; see also~~ *See* U.S.S.G. § 8B2.1(b)(5)(C) (an effectively working compliance program will have in place, and have publicized, "a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation").

- **Effectiveness of the Reporting Mechanism** – Does the company have an anonymous reporting mechanism and, if not, why not? How is the reporting mechanism publicized to the company's employees and other third parties? Has it been used? Does the company take measures to test whether employees are aware of the hotline and feel comfortable using it? How has the company assessed the seriousness of the

allegations it received? Has the compliance function had full access to reporting and investigative information?

- **Properly Scoped Investigations by Qualified Personnel** – How does the company determine which complaints or red flags merit further investigation? How does the company ensure that investigations are properly scoped? What steps does the company take to ensure investigations are independent, objective, appropriately conducted, and properly documented? How does the company determine who should conduct an investigation, and who makes that determination?

- **Investigation Response** – Does the company apply timing metrics to ensure responsiveness? Does the company have a process for monitoring the outcome of investigations and ensuring accountability for the response to any findings or recommendations?

- **Resources and Tracking of Results** – Are the reporting and investigating mechanisms sufficiently funded? How has the company collected, tracked, analyzed, and used information from its reporting mechanisms? Does the company periodically analyze the reports or investigation findings for patterns of misconduct or other red flags for compliance weaknesses? Does the company periodically test the effectiveness of the hotline, for example by tracking a report from start to finish?

E. Third Party Management

A well-designed compliance program should apply risk-based due diligence to its third-party relationships. Although the need for, and degree of, appropriate due diligence may vary based on the size and nature of the company, transaction, and third party, prosecutors should assess the extent to which the company has an understanding of the qualifications and associations of third-party partners, including the agents, consultants, and distributors that are commonly used to conceal misconduct, such as the payment of bribes to foreign officials in international business transactions.

Prosecutors should also assess whether the company knows the business rationale for needing the third party in the transaction, and the risks posed by third-party partners, including the third-party partners' reputations and relationships, if any, with foreign officials. For example, a prosecutor should analyze whether the company has ensured that contract terms with third parties specifically describe the services to be performed, that the third party is actually performing the work, and that its compensation is commensurate with the work being provided in that industry and geographical region. Prosecutors should further assess whether the

company engaged in ongoing monitoring of the third-party relationships, be it through updated due diligence, training, audits, and/or annual compliance certifications by the third party.

In sum, a company's third-party management practices are a factor that prosecutors should assess to determine whether a compliance program is in fact able to "detect [and prevent] the particular types of misconduct most likely to occur in a particular corporation's line of business." JM ~~928.800~~9-28.800.

- **Risk-Based and Integrated Processes** – How has the company's third-party management process corresponded to the nature and level of the enterprise risk identified by the company? How has this process been integrated into the relevant procurement and vendor management processes?

- **Appropriate Controls** – How does the company ensure there is an appropriate business rationale for the use of third parties? If third parties were involved in the underlying misconduct, what was the business rationale for using those third parties? What mechanisms exist to ensure that the contract terms specifically describe the services to be performed, that the payment terms are appropriate, that the described contractual work is performed, and that compensation is commensurate with the services rendered?

- **Management of Relationships** – How has the company considered and analyzed the compensation and incentive structures for third parties against compliance risks? How does the company monitor its third parties? Does the company have audit rights to analyze the books and accounts of third parties, and has the company exercised those rights in the past? How does the company train its ~~third party~~third-party relationship managers

about compliance risks and how to manage them? How does the company incentivize compliance and ethical behavior by third parties? Does the company engage in risk management of third parties throughout the lifespan of the relationship, or primarily during the onboarding process?

Real Actions and Consequences – Does the company track red flags that are identified from due diligence of third parties and how those red flags are addressed? Does the company keep track of third parties that do not pass the company's due diligence or that are terminated, and does the company take steps to ensure that those third parties are not hired or re-hired at a later date? If third parties were involved in the misconduct at issue in the investigation, were red flags identified from the due diligence or after hiring the third party, and how were they resolved? Has a similar third party been suspended, terminated, or audited as a result of compliance issues?

~~U.S. Department of Justice~~
~~Criminal Division~~

~~Evaluation of Corporate Compliance Programs~~

~~(Updated June 2020)~~

F. Mergers and Acquisitions (M&A)

A well-designed compliance program should include comprehensive due diligence of any acquisition targets, as well as a process for timely and orderly integration of the acquired entity into existing compliance program structures and internal controls. Pre-M&A due diligence, where possible, enables the acquiring company to evaluate more accurately each target's value and negotiate for the costs of any corruption or misconduct to be borne by the target. Flawed or incomplete pre- or post-acquisition due diligence and integration can allow misconduct to continue at the target company, causing resulting harm to a business's profitability and reputation and risking civil and criminal liability.

The extent to which a company subjects its acquisition targets to appropriate scrutiny is indicative of whether its compliance program is, as implemented, able to effectively enforce its internal controls and remediate misconduct at all levels of the organization.

- **Due Diligence Process** – Was the company able to complete pre-acquisition due diligence and, if not, why not? Was the misconduct or the risk of misconduct identified during due diligence? Who conducted the risk review for the acquired/merged entities and how was it done? What is the M&A due diligence process generally?

- **Integration in the M&A Process** – How has the compliance function been integrated into the merger, acquisition, and integration process?

- **Process Connecting Due Diligence to Implementation** – What has been the company's process for tracking and remediating misconduct or misconduct risks identified during the due diligence process? What has been the company's process for implementing compliance policies and procedures, and conducting post-acquisition audits, at newly acquired entities?

U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

(Updated March 2023)

II. Is the Corporation's Compliance Program Adequately Resourced and Empowered to Function Effectively?

Even a well-designed compliance program may be unsuccessful in practice if implementation is lax, under-resourced, or otherwise ineffective. Prosecutors are instructed to probe specifically whether a compliance program is a "paper program" or one "implemented, resourced, reviewed, and revised, as appropriate, in an effective manner." JM 9-28.800. In this regard, prosecutors should evaluate a corporation's method for assessing and addressing applicable risks and designing appropriate controls to manage these risks. In addition, prosecutors should determine "whether the corporation has provided for a staff sufficient to audit, document, analyze, and utilize the results of the corporation's compliance efforts." JM 9-28.800. Prosecutors should also determine "whether the corporation's employees are adequately informed about the compliance program and are convinced of the corporation's

commitment to it." JM 9-28.800; *see also* JM 9-47.120(2)(c) (criteria for an effective compliance program include "[t]he company's culture of compliance, including awareness among employees that any criminal conduct, including the conduct underlying the investigation, will not be tolerated").

A. Commitment by Senior and Middle Management

Beyond compliance structures, policies, and procedures, it is important for a company to create and foster a culture of ethics and compliance with the law at all levels of the company. The effectiveness of a compliance program requires a high-level commitment by company leadership to implement a culture of compliance from the middle and the top.

The company's top leaders – the board of directors and executives – set the tone for the rest of the company. Prosecutors should examine the extent to which senior management have clearly articulated the company's ethical standards, conveyed and disseminated them in clear and unambiguous terms, and demonstrated rigorous adherence by example. Prosecutors should also examine how middle management, in turn, have reinforced those standards and encouraged employees to abide by them. *See* U.S.S.G. § 8B2.1(b)(2)(A)-(C) (the company's "*governing authority* shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight" of it; "[*h*]*igh-level personnel* ... shall ensure that the organization has an effective compliance and ethics program" (emphasis added)).

- **Conduct at the Top** – How have senior leaders, through their words and actions, encouraged or discouraged compliance, including the type of misconduct involved in the investigation? What concrete actions have they taken to demonstrate leadership in the company's compliance and remediation efforts? How have they modelled proper behavior to subordinates? Have managers tolerated greater compliance risks in pursuit of new business or greater revenues? Have managers encouraged employees to act unethically to achieve a business objective, or impeded compliance personnel from effectively implementing their duties?

- **Shared Commitment** – What actions have senior leaders and middle-management stakeholders (*e.g.*, business and operational managers, finance, procurement, legal, human resources) taken to demonstrate their commitment to compliance or compliance personnel, including their remediation efforts? Have they persisted in that commitment in the face of competing interests or business objectives?

- **Oversight** – What compliance expertise has been available on the board of directors? Have the board of directors and/or external auditors held executive or private sessions with the compliance and control functions? What types of information have

the board of directors and senior management examined in their exercise of oversight in the area in which the misconduct occurred?

B. Autonomy and Resources

Effective implementation also requires those charged with a compliance program's day-to-day oversight to act with adequate authority and stature. As a threshold matter, prosecutors should evaluate how the compliance program is structured. Additionally, prosecutors should address the sufficiency of the personnel and resources within the compliance function, in particular, whether those responsible for compliance have: (1) sufficient seniority within the organization; (2) sufficient resources, namely, staff to effectively undertake the requisite auditing, documentation, and analysis; and (3) sufficient autonomy from management, such as direct access to the board of directors or the board's audit committee. The sufficiency of each factor, however, will depend on the size, structure, and risk profile of the particular company. "A large organization generally shall devote more formal operations and greater resources . . . than shall a small organization." Commentary to U.S.S.G. § 8B2.1 note 2(C). By contrast, "a small organization may [rely on] less formality and fewer resources." *Id.* Regardless, if a compliance program is to be truly effective, compliance personnel must be empowered within the company.

Prosecutors should evaluate whether ~~"~~internal audit functions [are] conducted at a level sufficient to ensure their independence and accuracy,~~"~~ as an indicator of whether compliance personnel are in fact empowered and positioned to ~~"~~effectively detect and prevent misconduct.~~"~~ ~~JM 9-28.800~~. Prosecutors should also evaluate "[t]he resources the company has dedicated to compliance," "[t]he quality and experience of the personnel involved in compliance, such that they can understand and identify the transactions and activities that pose a potential risk," and "[t]he authority and independence of the compliance function and the availability of compliance expertise to the board." JM 9-47.120(2)(c); *see also* ~~JM 9-28.800 (instructing prosecutors to evaluate whether "the directors established an information and reporting system in the organization reasonably designed to provide management and directors with timely and accurate information sufficient to allow them to reach an informed decision regarding the organization's compliance with the law");~~ U.S.S.G. § 8B2.1(b)(2)(C) (those with "day-to-day operational responsibility" shall have "adequate resources, appropriate authority and direct access to the governing authority or an appropriate subgroup of the governing authority").

- **Structure** – Where within the company is the compliance function housed (e.g., within the legal department, under a business function, or as an independent function reporting to the CEO and/or board)? To whom does the compliance function report? Is the compliance function run by a designated chief compliance officer, or another executive

within the company, and does that person have other roles within the company? Are compliance personnel dedicated to compliance responsibilities, or do

they have other, non-compliance responsibilities within the company? Why has the company chosen the compliance structure it has in place? What are the reasons for the structural choices the company has made?

- **Seniority and Stature** – How does the compliance function compare with other strategic functions in the company in terms of stature, compensation levels, rank/title, reporting line, resources, and access to key decision-makers? What has been the turnover rate for compliance and relevant control function personnel? What role has compliance played in the company's strategic and operational decisions? How has the company responded to specific instances where compliance raised concerns? Have there been transactions or deals that were stopped, modified, or further scrutinized as a result of compliance concerns?

- **Experience and Qualifications** – Do compliance and control personnel have the appropriate experience and qualifications for their roles and responsibilities? Has the level of experience and qualifications in these roles changed over time? How does the company invest in further training and development of the compliance and other control personnel? Who reviews the performance of the compliance function and what is the review process?

- **Funding and Resources** – Has there been sufficient staffing for compliance personnel
to effectively audit, document, analyze, and act on the results of the compliance efforts? Has the company allocated sufficient funds for the same? Have there been times when requests for resources by compliance and control functions have been denied, and if so, on what grounds?

- **Data Resources and Access** – Do compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions? Do any impediments exist that limit access to relevant sources of data and, if so, what is the company doing to address the impediments?

- **Autonomy** – Do the compliance and relevant control functions have direct reporting lines to anyone on the board of directors and/or audit committee? How often do they meet with directors? Are members of the senior management present for these meetings? How does the company ensure the independence of the compliance and control personnel?

U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

(Updated ~~June 2020~~March 2023)

- **Outsourced Compliance Functions** – Has the company outsourced all or parts of its compliance functions to an external firm or consultant? If so, why, and who is responsible for overseeing or liaising with the external firm or consultant? What level of access does the external firm or consultant have to company information? How has the effectiveness of the outsourced process been assessed?

C. ~~Incentives and Disciplinary Measures~~Compensation Structures and Consequence Management

Another hallmark of effective implementation of a compliance program is the establishment of incentives for compliance and disincentives for non-compliance. Prosecutors should assess whether the company has clear ~~disciplinary~~consequence management procedures (procedures to identify, investigate, discipline and remediate violations of law, regulation, or policy) in place, enforces them consistently across the organization, and ensures that the procedures are commensurate with

the violations. Prosecutors should also assess the extent to which the company's communications convey to its employees that unethical conduct will not be tolerated and will bring swift consequences, regardless of the position or title of the employee who engages in the conduct. *See* U.S.S.G. § 8B2.1(b)(5)(C) ("the organization's compliance program shall be promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct").

By way of example, ~~some companies have found that publicizing~~prosecutors may consider whether a company has publicized disciplinary actions internally, where appropriate and possible, which can have valuable deterrent effects. ~~At the same time, some companies have also found that~~ Prosecutors may also consider whether a company is tracking data relating to disciplinary actions to measure effectiveness of the investigation and consequence management functions. This can include monitoring the number of compliance-related allegations that are substantiated, the average (and outlier) times to complete a compliance investigation, and the effectiveness and consistency of disciplinary measures across the levels, geographies, units or departments of an organization.

The design and implementation of compensation schemes play an important role in fostering a compliance culture. Prosecutors may consider whether a company has incentivized compliance by designing compensation systems that defer or escrow certain compensation tied to conduct consistent with company values and policies. Some companies have also enforced contract provisions that permit the company to recoup previously awarded compensation if the recipient of such compensation is found to have engaged in or to be otherwise responsible for corporate wrongdoing. Finally, prosecutors may consider whether provisions for recoupment or reduction of compensation due to compliance violations or misconduct are maintained and enforced in accordance with company policy and applicable laws.

Compensation structures that clearly and effectively impose financial penalties for misconduct can deter risky behavior and foster a culture of compliance. At the same time,

providing positive incentives ~~– personnel~~, such as promotions, rewards, and bonuses for improving and developing a compliance program or demonstrating ethical leadership ~~– have driven~~, can drive compliance. ~~Some companies have even made compliance a significant metric for management bonuses and/or have~~Prosecutors should examine whether a company has made working on compliance a means of career advancement~~.~~, offered opportunities for managers and employees to serve as a compliance "champion", or made compliance a significant metric for management bonuses. In evaluating whether the compensation and consequence management schemes are indicative of a positive compliance culture, prosecutors should consider the following factors:

- **Human Resources Process** – Who participates in making disciplinary decisions, including for the type of misconduct at issue? How transparent has the company been with the design and implementation of its disciplinary process? In circumstances where an executive has been exited from the company on account of a compliance violation, how transparent has the company been with employees about the terms of the separation? Are the actual reasons for discipline communicated to employees in all cases? If not, why not? Is the same process followed for each instance of misconduct, and if not, why? ~~Are the actual reasons for discipline communicated to employees? If not, why not?~~Has the company taken steps to restrict disclosure or access to information about the disciplinary process? Are there legal or investigation-related reasons for restricting information, or have pre-textual reasons been provided to protect the company from whistleblowing or outside scrutiny?

- **Disciplinary Measures** – What types of disciplinary actions are available to management when it seeks to enforce compliance policies? Does the company have policies or procedures in place to recoup compensation that would not have been achieved but for misconduct attributable directly or indirectly to the executive or employee? What policies and practices does the company have in place to put employees on notice that they will not benefit from any potential fruits of misconduct? With respect to the particular misconduct at issue, has the company made good faith efforts to follow its policies and practices in this respect?

- **Consistent Application** – Have disciplinary actions and incentives been fairly and consistently applied across the organization? Does the compliance function monitor its investigations and resulting discipline to ensure consistency? Are there similar instances of misconduct that were treated disparately, and if so, why? What metrics does the company apply to ensure consistency of disciplinary measures across all geographies, operating units, and levels of the organization?

- **Financial Incentive System** – Has the company considered the impact of its financial

~~U.S. Department of Justice~~
~~Criminal Division~~

~~Evaluation of Corporate Compliance Programs~~

~~(Updated June 2020)~~

- ~~Incentive System – Has the company considered the implications of its~~rewards and other incentives ~~and rewards~~ on compliance? Has the company evaluated whether commercial targets are achievable if the business operates within a compliant and ethical manner? What role does the compliance function have in designing and awarding financial incentives at senior levels of the organization? How does the company incentivize compliance and ethical behavior? What percentage of executive

~~ethical behavior~~compensation is structured to encourage enduring ethical business objectives? Are the terms of bonus and deferred compensation subject to cancellation or recoupment, to the extent available under applicable law, in the event that non-compliant or unethical behavior is exposed before or after the award was issued? Does the company have a policy for recouping compensation that has been paid, where there has been misconduct? Have there been specific examples of actions taken (*e.g.*, promotions or awards denied, compensation recouped or deferred compensation cancelled) as a result of compliance and ethics considerations? ~~Who determines the compensation, including bonuses, as well as discipline and promotion of compliance personnel?~~

- **Effectiveness** – How has the company ensured effective consequence management of compliance violations in practice? What insights can be taken from the management of a company's hotline that provide indicia of its compliance culture or its management of hotline reports? How do the substantiation rates compare for similar types of reported wrongdoing across the company (*i.e.* between two or more different states, countries, or departments) or compared to similarly situated companies, if known? Has the company undertaken a root cause analysis into areas where certain conduct is comparatively over or under reported? What is the average time for completion of investigations into hotline reports and how are investigations that are addressed inconsistently managed by the responsible department? What percentage of the compensation awarded to executives who have been found to have engaged in wrongdoing has been subject to cancellation or recoupment for ethical violations? Taking into account the relevant laws and local circumstances governing the relevant parts of a compensation scheme, how has the organization sought to enforce breaches of compliance or penalize ethical lapses? How much compensation has in fact been impacted (either positively or negatively) on account of compliance-related activities?

III. Does the Corporation's Compliance Program Work in Practice?

The Principles of Federal Prosecution of Business Organizations require prosecutors to assess "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision." JM 9-28.300. Due to the backward-looking nature of the first inquiry, one of the most difficult questions prosecutors must answer in evaluating a compliance program following misconduct is whether the program was working effectively at the time of the offense, especially where the misconduct was not immediately detected.

In answering this question, it is important to note that the existence of misconduct does not, by itself, mean that a compliance program did not work or was ineffective at the time of the offense. *See* U.S.S.G. § 8B2.1(a) ("[t]he failure to prevent or detect the instant offense does not mean that the program is not generally effective in preventing and deterring misconduct"). Indeed, "[t]he Department recognizes that no compliance program can ~~ever~~ prevent all criminal activity by a corporation's employees." JM 9-28.800. Of course, if a compliance program did effectively identify misconduct, including allowing for timely remediation and self-reporting, a prosecutor

14

should view the occurrence as a strong indicator that the compliance program was working effectively.

In assessing whether a company's compliance program was effective at the time of the misconduct, prosecutors should consider whether and how the misconduct was detected, what investigation resources were in place to investigate suspected misconduct, and the nature and thoroughness of the company's remedial efforts.

To determine whether a company's compliance program is working effectively at the time of a charging decision or resolution, prosecutors should consider whether the program evolved over time to address existing and changing compliance risks. Prosecutors should also consider whether the company undertook an adequate and honest root cause analysis to understand both what contributed to the misconduct and the degree of remediation needed to prevent similar events in the future.

~~U.S. Department of Justice~~
~~Criminal Division~~

~~Evaluation of Corporate Compliance Programs~~

~~(Updated June 2020)~~

~~For example, prosecutors should consider, among other factors, "whether the corporation has made significant investments in, and improvements to, its corporate compliance program and internal controls systems" and "whether remedial improvements to the compliance program and internal controls have been tested to demonstrate that they would prevent or detect similar misconduct in the future." Benczkowski Memo at 2 (observing that "[w]here a corporation's compliance program and controls are demonstrated to be effective and appropriately resourced at the time of resolution, a monitor will not likely be necessary").~~

A. Continuous Improvement, Periodic Testing, and Review

One hallmark of an effective compliance program is its capacity to improve and evolve. The actual implementation of controls in practice will necessarily reveal areas of risk and potential adjustment. A company's business changes over time, as do the environments in which it operates, the nature of its customers, the laws that govern its actions, and the applicable industry standards. Accordingly, prosecutors should consider whether the company has engaged in meaningful efforts to review its compliance program and ensure that it is not stale. Some companies survey employees to gauge the compliance culture and evaluate the strength of controls, and/or conduct periodic audits to ensure that controls are functioning well, though the nature and frequency of evaluations may depend on the company's size and complexity.

Prosecutors may reward efforts to promote improvement and sustainability. In evaluating whether a particular compliance program works in practice, prosecutors should consider "revisions to corporate compliance programs in light of lessons learned." JM 9-28.800; *see also* JM ~~9-47-120~~9-47120(2)(c) (looking to "[t]he auditing of the compliance program to assure its effectiveness"). Prosecutors should likewise look to whether a company has taken "reasonable steps" to "ensure that the organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct," and "evaluate periodically the effectiveness of the organization's" program. U.S.S.G. § 8B2.1(b)(5). Proactive efforts like these may not only be rewarded in connection with the form of any resolution or prosecution (such as through remediation credit or a lower applicable fine range under the Sentencing Guidelines), but more importantly, may avert problems down the line.

- **Internal Audit** – What is the process for determining where and how frequently internal audit will undertake an audit, and what is the rationale behind that process? How are audits carried out? What types of audits would have identified issues relevant to the misconduct? Did those audits occur and what were the findings? What types of relevant audit findings and remediation progress have been reported to management

and the board on a regular basis? How have management and the board followed up? How often does internal audit conduct assessments in high-risk areas?

~~U.S. Department of Justice~~
~~Criminal Division~~

~~Evaluation of Corporate Compliance Programs~~

~~(Updated June 2020)~~

- **Control Testing** – Has the company reviewed and audited its compliance program in the area relating to the misconduct? More generally, what testing of controls, collection and analysis of compliance data, and interviews of employees and third parties does the company undertake? How are the results reported and action items tracked?

- **Evolving Updates** – How often has the company updated its risk assessments and reviewed its compliance policies, procedures, and practices? Has the company undertaken a gap analysis to determine if particular areas of risk are not sufficiently addressed in its policies, controls, or training? What steps has the company taken to determine whether policies/procedures/practices make sense for particular business segments/subsidiaries? Does the company review and adapt its compliance program based upon lessons learned from its own misconduct and/or that of other companies facing similar risks?

- **Culture of Compliance** – How often and how does the company measure its culture of compliance? How does the company's hiring and incentive structure reinforce its commitment to ethical culture? Does the company seek input from all levels of employees to determine whether they perceive senior and middle management's commitment to compliance? What steps has the company taken in response to its measurement of the compliance culture?

B. Investigation of Misconduct

Another hallmark of a compliance program that is working effectively is the existence of a well-functioning and appropriately funded mechanism for the timely and thorough investigations of any allegations or suspicions of misconduct by the company, its employees, or agents. An effective investigations structure will also have an established means of documenting the company's response, including any disciplinary or remediation measures taken.

- **Properly Scoped Investigation by Qualified Personnel** – How has the company ensured that the investigations have been properly scoped, and were independent, objective, appropriately conducted, and properly documented?

- **Response to Investigations** – Have the company's investigations been used to identify root causes, system vulnerabilities, and accountability lapses, including among supervisory managers and senior executives? What has been the process for responding to investigative findings? How high up in the company do investigative findings go?

U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

(Updated ~~June 2020~~March 2023)

- **Independence and Empowerment** – Is compensation for employees who are responsible for investigating and adjudicating misconduct structured in a way that ensures the compliance team is empowered to enforce the policies and ethical values of the company? Who determines the compensation, including bonuses, as well as discipline and promotion of compliance personnel or others within the organization that have a role in the disciplinary process generally?

Messaging applications have become ubiquitous in many markets and offer important platforms for companies to achieve growth and facilitate communication. In evaluating a corporation's policies and mechanisms for identifying, reporting, investigating, and remediating potential misconduct and violations of law, prosecutors should consider a corporation's policies and procedures governing the use of personal devices, communications platforms, and messaging applications, including ephemeral messaging applications. Policies governing such applications should be tailored to the corporation's risk profile and specific business needs and ensure that, as appropriate and to the greatest extent possible, business-related electronic data and communications are accessible and amenable to preservation by the company. Prosecutors should consider how the policies and procedures have been communicated to employees, and whether the corporation has enforced the policies and procedures on a regular and consistent basis in practice. In conducting this evaluation, prosecutors should consider the following factors:

- **Communication Channels** – What electronic communication channels do the company and its employees use, or allow to be used, to conduct business? How does that practice vary by jurisdiction and business function, and why? What mechanisms has the company put in place to manage and preserve information contained within each of the electronic communication channels? What preservation or deletion settings are available to each employee under each communication channel, and what do the company's policies require with respect to each? What is the rationale for the company's approach to determining which communication channels and settings are permitted?

- **Policy Environment** – What policies and procedures are in place to ensure that communications and other data is preserved from devices that are replaced? What are the relevant code of conduct, privacy, security, and employment laws or policies that govern the organization's ability to ensure security or monitor/access business-related communications? If the company has a "bring your own device" (BYOD) program, what are its policies governing preservation of and access to corporate data and communications stored on personal devices—including data contained within messaging platforms—and what is the rationale behind those policies? How have the company's data retention and business conduct policies been applied and enforced with respect to personal devices and messaging applications? Do the organization's policies permit the company to review business communications on BYOD and/or messaging applications? What exceptions or limitations to these policies have been permitted by

the organization? If the company has a policy regarding whether employees should transfer messages, data, and information from private phones or messaging applications onto company record-keeping systems in order to preserve and retain them, is it being followed in practice, and how is it enforced?

- **Risk Management** – What are the consequences for employees who refuse the company access to company communications? Has the company ever exercised these rights? Has the company disciplined employees who fail to comply with the policy or the requirement that they give the company access to these communications? Has the use of personal devices or messaging applications—including ephemeral messaging applications—impaired in any way the organization's compliance program or its ability to conduct internal investigations or respond to requests from prosecutors or civil enforcement or regulatory agencies? How does the organization manage security and exercise control over the communication channels used to conduct the organization's affairs? Is the organization's approach to permitting and managing communication channels, including BYOD and messaging applications, reasonable in the context of the company's business needs and risk profile?

C. Analysis and Remediation of Any Underlying Misconduct

Finally, a hallmark of a compliance program that is working effectively in practice is the extent to which a company is able to conduct a thoughtful root cause analysis of misconduct and timely and appropriately remediate to address the root causes.

Prosecutors evaluating the effectiveness of a compliance program are instructed to reflect back on "the extent and pervasiveness of the criminal misconduct; the number and level of the corporate employees involved; the seriousness, duration, and frequency of the misconduct; and any remedial actions taken by the corporation, including, for example, disciplinary action against past violators uncovered by the prior compliance program, and revisions to corporate compliance programs in light of lessons learned." JM 9-28.800; *see also* JM 9-47.120(3)(c) ("to receive full credit for timely and appropriate remediation" under the FCPA Corporate Enforcement Policy, a company should demonstrate "a root cause analysis" and, where appropriate, "remediation to address the root causes").

Prosecutors should consider "any remedial actions taken by the corporation, including, for example, disciplinary action against past violators uncovered by the prior compliance program." JM 98-28.800; *see also* JM 9-47-120(2)(c) (looking to "[a]ppropriate discipline of employees, including those identified by the company as responsible for the misconduct, either through direct participation or failure in oversight, as well as those with supervisory authority over the area in which the criminal conduct occurred" and "any additional steps that demonstrate recognition of the seriousness of the misconduct, acceptance of responsibility for it, and the implementation of measures to reduce the risk of repetition of such misconduct, including measures to identify future risk").

- **Root Cause Analysis** – What is the company's root cause analysis of the misconduct at issue? Were any systemic issues identified? Who in the company was involved in making the analysis?

- **Prior Weaknesses** – What controls failed? If policies or procedures should have prohibited the misconduct, were they effectively implemented, and have functions that had ownership of these policies and procedures been held accountable?

- **Payment Systems** – How was the misconduct in question funded (*e.g.*, purchase orders, employee reimbursements, discounts, petty cash)? What processes could have prevented or detected improper access to these funds? Have those processes been improved?

~~U.S. Department of Justice~~
~~Criminal Division~~

~~Evaluation of Corporate Compliance Programs~~

~~(Updated June 2020)~~

- **Vendor Management** – If vendors were involved in the misconduct, what was the process for vendor selection and did the vendor undergo that process?

- **Prior Indications** – Were there prior opportunities to detect the misconduct in question, such as audit reports identifying relevant control failures or allegations, complaints, or investigations? What is the company's analysis of why such opportunities were missed?

- **Remediation** – What specific changes has the company made to reduce the risk that the same or similar issues will ~~not~~ occur in the future? What specific remediation has addressed the issues identified in the root cause and missed opportunity analysis?

- **Accountability** – What disciplinary actions did the company take in response to the misconduct and were they timely? Were managers held accountable for misconduct that occurred under their supervision? Did the company consider disciplinary actions for failures in supervision? What is the company's record (*e.g.*, number and types of disciplinary actions) on employee discipline relating to the types of conduct at issue? Has the company ever terminated or otherwise disciplined anyone (reduced or eliminated bonuses, issued a warning letter, etc.) for the type of misconduct at issue? Did the company take any actions to recoup or reduce compensation for responsible employees to the extent practicable and available under applicable law?

[1] Many of the topics also appear in the following resources:

U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

(Updated March 2023)

- Justice Manual ("JM")
  - JM 9-28.000 Principles of Federal Prosecution of Business Organizations, Justice Manual ("JM"), *available at* https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations.
  - JM 9-47.120 ~~FCPA~~and the Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy, *available at* ~~https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977#9-47.120.~~ https://www.justice.gov/criminal-fraud/file/1562831/download.
- Chapter 8 – Sentencing of Organizations - United States Sentencing Guidelines ("U.S.S.G."), *available at* ~~https://www.ussc.gov/guidelines/2018-guidelines-manual/2018-chapter-8#NaN.~~ https://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2021/CHAPTER_8.pdf.

~~U.S. Department of Justice~~
~~Criminal Division~~

~~Evaluation of Corporate Compliance Programs~~

~~(Updated June 2020)~~

- Memorandum entitled "Selection of Monitors in Criminal Division Matters," issued by Assistant Attorney General Brian Benczkowski on October 11, 2018, *available at* https://www.justice.gov/criminal-fraud/file/1100366/download; updated Memorandum entitled "Selection of Monitors in Criminal Division Matters," issued by Assistant Attorney General Kenneth A. Polite, Jr., on March 1, 2023, *available at* https://www.justice.gov/criminal-fraud/file/1100366/download.

- Criminal Division corporate resolution agreements, *available at* https://www.justice.gov/news (the Department of Justice's ("DOJ") Public Affairs website contains press releases for all Criminal Division corporate resolutions which contain links to charging documents and agreements).

- A Resource Guide to the U.S. Foreign Corrupt Practices Act (2d ed.) ("FCPA Guide"), published in ~~November 2012~~July 2020 by the DOJ and the Securities and Exchange Commission ("SEC"), *available at* ~~https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf.~~ https://www.justice.gov/criminal-fraud/file/1292051/download.

- ~~Good Practice Guidance on Internal Controls, Ethics, and Compliance, adopted~~Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions, amended by the Organization for Economic ~~Co-operation~~Cooperation and Development ("OECD") Council on ~~February 18, 2010~~November 25, 2021, *available at* ~~https://www.oecd.org/daf/anti-bribery/44884389.pdf~~https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0378.

- Anti-Corruption Ethics and Compliance Handbook for Business ("OECD Handbook"), published in 2013 by OECD, United Nations Office on Drugs and Crime, and the World Bank, *available at* https://www.oecd.org/corruption/Anti-CorruptionEthicsComplianceHandbook.pdf.

- Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations, published in July 2019 by DOJ's Antitrust Division, *available at* https://www.justice.gov/atr/page/file/1182001/download.

- A Framework for OFAC Compliance Commitments, published in May 2019 by the Department of the Treasury's Office of Foreign Assets Control ("OFAC"), *available at https://www.treasury.gov/resource-center/sanctions/Documents/framework _ofac_cc.pdf.*

[2] Prosecutors should consider whether certain aspects of a compliance program may be impacted by foreign law. Where a company asserts that it has structured its compliance program in a particular way or has made a compliance decision based on requirements of foreign law, prosecutors should ask the company the basis for the company's conclusion about foreign law, and how the company has addressed the issue to maintain the integrity and effectiveness of its compliance program while still abiding by foreign law.

[3] As discussed in the Justice Manual, many companies operate in complex regulatory environments outside the normal experience of criminal prosecutors. JM 9-28.000. For example, financial institutions such as banks, subject to the Bank Secrecy Act statute and regulations,

require prosecutors to conduct specialized analyses of their compliance programs in the context of their anti-money laundering requirements. Consultation with the Money Laundering and Asset Recovery Section is recommended when reviewing AML compliance. *See* https://www.justice.gov/criminal-mlars~~.~~ Prosecutors may also wish to review guidance published by relevant federal and state agencies. *See* Federal Financial Institutions Examination Council/Bank Secrecy Act/Anti-Money Laundering Examination Manual, *available at* ~~https://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm).~~ https://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm).

Summary report: Litera Compare for Word 11.7.0.54 Document comparison done on 3/5/2024 1:19:38 PM	
Style name: Default Style	
Intelligent Table Comparison: Active	
Original filename: DOJ Compliance 2020.docx	
Modified filename: DOJ Compliance 2023.docx	
Changes:	
Add	217
~~Delete~~	210
~~Move From~~	49
Move To	49
Table Insert	0
~~Table Delete~~	0
Table moves to	0
~~Table moves from~~	0
Embedded Graphics (Visio, ChemDraw, Images etc.)	0
Embedded Excel	0
Format changes	0
Total Changes:	525

About Akin

About Akin

An Overview of Akin

Akin is a global elite law firm providing innovative legal services and business solutions to individuals and institutions. With 17 offices worldwide and more than 900 lawyers and professionals, we are among the world's largest law firms, yet we strive to provide every client focused and consistent attention.

Distinguished by the breadth of our experience and capabilities, our commitment to client service is supported by a culture rooted in collaboration and caring. Every day, our professionals tackle complex and highly consequential legal engagements with keen commercial awareness and a strategic alignment with our clients' business goals. Akin is known for its strength in disputes, investigations and high-stakes appellate work, leadership in transformative transactions and depth in lobbying and public policy. Serving clients in more than 250 areas that range from the traditional, such as disputes, corporate and finance, to the cutting edge, such as biotechnology, renewable energy and cybersecurity, we are committed to creating, expanding and protecting our clients' assets and interests.

Through our network of domestic and international offices, we advise companies across myriad industries in both mature and emerging markets. Akin professionals possess a sharp understanding of the intangible factors in economic and political infrastructures, combining it with firsthand government experience at the highest levels around the world. Armed with our advice, clients can grow and thrive in the global marketplace.

80+
COUNTRIES WHERE WE HANDLE MATTERS

17
OFFICES AROUND THE WORLD

140+
COUNTRIES ARE HOME TO OUR CLIENTS

Akin's Life Sciences Practice

Pharmaceutical Practice Overview

Every day our clients are developing new and exciting products that shape the future of health care and wellness for patients and consumers. While making important advances in medical products and food, they also face multiple challenges. We help clients overcome these hurdles by engaging with the U.S. Food and Drug Administration (FDA) and other global and state regulators. We also advise clients on the best way to secure investments for new research and development and to manage the ongoing risk of high-stakes investigations, enforcement actions and recalls that could potentially result in litigation.

From your initial concept until your new product is in the hands of consumers, our team will work with you during all stages of the product's life cycle. To do this, we guide you through a product's research and development, review and approval, commercialization, post-market obligations and modifications. We can handle any compliance or enforcement challenges that arise. We also make sure that your business transactions and compliance programs adhere to all applicable laws and FDA regulations.

By combining our lawyers' in-depth and firsthand knowledge of FDA regulations and public policy advocacy with the resources of a full-service global law firm, our food, drug and device practice effectively:

- Provides regulatory and strategic advice to clients during product development, the application and approval process, post-market requirements, recalls and FDA 483s.
- Advises clients on pharmaceutical compliance program requirements, policies, implementation and best practices as well as internal and external government investigations.
- Advises clients on FDA-related compliance issues and represents clients in enforcement actions brought by the FDA, DOJ and other authorities.
- Performs due diligence and develops agreements relating to investments and transactions in FDA-regulated companies and products.
- Develops and executes advocacy strategies for policy and legislative reforms relating to FDA-regulated products.
- Advises companies on the development and commercialization of both large and small molecules, orphan drug and other exclusivities, priority review vouchers (PRVs) and rare diseases.

Creates strategies with clients on drug pricing, reimbursement and reporting, including the potential impact of the Inflation Reduction Act's (IRA) drug price negotiation program on strategic pipeline development decisions, commercialization and litigation matters.

Akin's Life Sciences Practice

Our Health Care & Life Sciences Regulatory Specialties

Transactions Overview

We combine our skills to help organizations successfully bring their health care innovations and food products to market and lay the foundation for long-term success. We work with investors, financial institutions and companies on corporate transactions and other partnership. Our clients include companies that rely on us to analyze, draft and negotiate licensing agreements relating to FDA-regulated products and data supporting marketing submissions.

Our integrated transactions teams have the skill and broad experience to help life science businesses, health care companies, their investors and other industry participants chart a path to success. We combine highly experienced corporate transactional attorneys with members of our health care & life sciences regulatory practice to bring a comprehensive approach to our clients' projects.

For deals subject to antitrust scrutiny, experts from our antitrust and state attorneys general practices help clients navigate state and federal regulatory review processes and offer strategic counsel to maximize chances of success.

We represent leading drug and device manufacturers, health systems, hospitals, investors and lenders in complex acquisitions, divestitures, mergers, joint ventures, financings and restructurings. Our lawyers have assisted in high-profile transactions stemming from consolidation trends, realignments, cost and quality control initiatives, innovative technology developments and an increased interest by private-equity investors in health care providers and the wide variety of companies servicing the industry.

In addition, our royalty monetization team focuses on representing clients in the purchase and sale of, or financing backed by, interests in royalty and synthetic streams relating to life sciences and pharmaceutical products. We have deep experience in transactions that involve contingent considerations such as royalty payments and milestone payments.

Contact

Craig B. Bleifer

Partner

cbleifer@akingump.com
New York
T +1 212.872.8184

- Experienced executive with more than 20 years of in-house experience in the pharmaceutical industry. Former Senior Vice President (VP) and General Counsel, Novo Nordisk, and former Senior VP & General Counsel, Daiichi Sankyo.
- Counsels health care and life sciences clients on a range of compliance, policy, regulatory and corporate matters involving the FDA, Centers for Medicare & Medicaid Services (CMS) and HHS OIG.
- Negotiates transactional documents for licenses, co-promotion/co-development, outsourcing, manufacturing and mergers and acquisitions (M&A) agreements between life sciences companies as well as M&A and investment agreements on behalf of PE and venture capital (VC) firms.

Locations

United States

Boston
33 Arch Street
Suite 2500
Boston, MA 02110
T +1 617.535.6161

Dallas
2300 N. Field Street
Suite 1800
Dallas, TX 75201-2481
T +1 214.969.2800

Fort Worth
201 Main Street
Suite 1600
Fort Worth, TX 76102
T +1 817.886.5060

Houston
1111 Louisiana Street
44th Floor
Houston, TX 77002-5200
T +1 713.220.5800

Irvine
4 Park Plaza
Suite 1900
Irvine, CA 92614-2585
T +1 949.885.4100

Los Angeles
1999 Avenue of the Stars
Suite 600
Los Angeles, CA 90067-6022
T +1 310.229.1000

Philadelphia
1735 Market Street
12th Floor
Philadelphia, PA 19103-7501
T +1 215.965.1200

New York
One Bryant Park
Bank of America Tower
New York, NY 10036-6745
T +1 212.872.1000

San Antonio
112 E. Pecan Street
Suite 1010
San Antonio, TX 78205-1512
T +1 210.281.7000

San Francisco
100 Pine Street
Suite 3200
San Francisco, CA 94111-5218
T +1 415.765.9500

Washington, D.C.
Robert S. Strauss Tower
2001 K Street, N.W.
Washington, DC 20006-1037
T +1 202.887.4000

Asia

Hong Kong
Units 1801-08 & 10
18th Floor Gloucester Tower
The Landmark
15 Queen's Road Central
Central, Hong Kong
T +852 3694.3000

Singapore
2 Shenton Way
#16-01 SGX Centre 1
Singapore 068804
T +65 6579.9000

Europe

Geneva
54 Quai Gustave Ador
1207 Geneva, Switzerland
T +41 22.888.2000

London
Ten Bishops Square
Eighth Floor
London, E1 6EG United Kingdom
T +44 20.7012.9600

Middle East

Abu Dhabi
Abu Dhabi Global Market Square
Al Sila Tower
21st Floor
P.O. Box 55069
Abu Dhabi, UAE
T +971 2.406.8500

Dubai
ICD Brookfield Place
Level 40
Al Mustaqbal Street
DIFC
Dubai, UAE
T +971 4.317.3000

Akin

Akin is a leading global law firm providing innovative legal services and business solutions to individuals and institutions. Founded in 1945 by Richard Gump and Robert Strauss with the guiding vision that commitment, excellence and integrity would drive its success, the firm focuses on building lasting and mutually beneficial relationships with its clients. Our firm's clients range from individuals to corporations and nations. We offer clients a broad-spectrum approach, with over 85 practices that range from traditional strengths such as appellate, corporate and public policy to 21st century concentrations such as climate change, intellectual property litigation and national security.