U.S. Department of Health and Human Services

Office of Inspector General

General Compliance Program Guidance

November 2023

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.

Table of Contents

I. Introduction

Who We Are

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

Existing Compliance Program Guidance

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

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.

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.

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

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).

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.

- 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?

- 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.

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.

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.

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.

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.

- 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.

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).

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).

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).

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.

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).

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.

Tip **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).

- 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).

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.

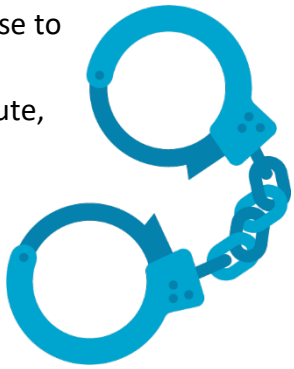
Many State Medicaid programs now have their own exclusion authorities and maintain their own State exclusion lists. If an entity employs or contracts or otherwise engages with individuals or entities excluded from a State Medicaid program in which it participates, the

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

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.

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.

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

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.

7 Elements of a Successful Compliance Program

1. Written Policies and Procedures
2. Compliance Leadership and Oversight
3. Training and Education
4. Effective Lines of Communication with the Compliance Officer and Disclosure Program
5. Enforcing Standards: Consequences and Incentives
6. Risk Assessment, Auditing, and Monitoring
7. Responding to Detected Offenses and Developing Corrective Action Initiatives

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.

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.

Tip **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.

Tip **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.

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).

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

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;

- 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.

- 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.

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.

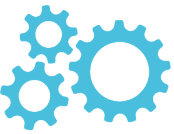
Coordination and communication are the compliance officer's key tools for planning, implementing, and monitoring an effective compliance program. The compliance officer should strive to develop, and the entity should strive to promote, productive working relationships with organizational leaders. Coordinating 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;

- 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.

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.

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)

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

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'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.

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

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

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.

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.

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.

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.

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.

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.

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.

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.

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

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.

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.)

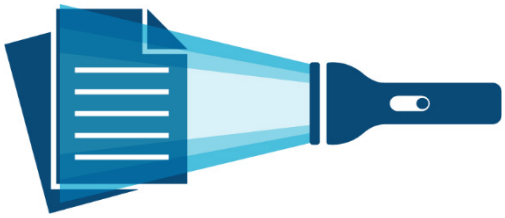
Although conducting formal risk assessments may be new to many compliance programs, risk assessments are an integral part of the fiscal internal control process and to enterprise risk management, and are required for recipients of federal awards. Compliance Committees should educate themselves on risk 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.

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

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.

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.

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.

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.

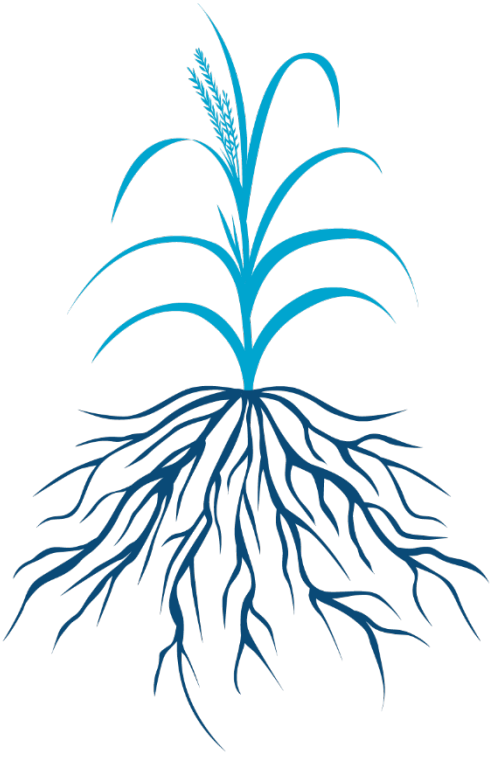
3. Implementing Corrective Action Initiatives

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).

SECTION IV
Compliance Program Adaptations for Small and Large Entities

Return to TOC

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.

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.

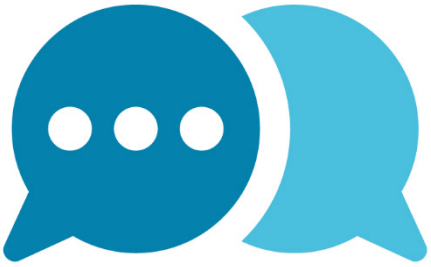
3. Open Lines of Communication

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

- 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

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.

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.

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.

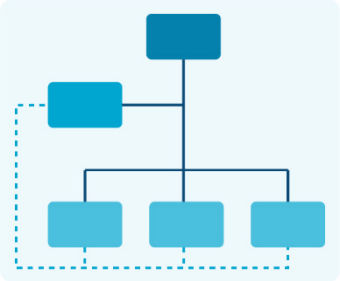
The chief compliance officer should consider the varying skills that may be needed within the department, such as auditors, investigators, clinicians, and data experts, to operate effectively, and whether use of specialized consultants or part-time employees may be beneficial. If the large organization 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.

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.

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).

SECTION V
Other Compliance Considerations

Return to TOC

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.

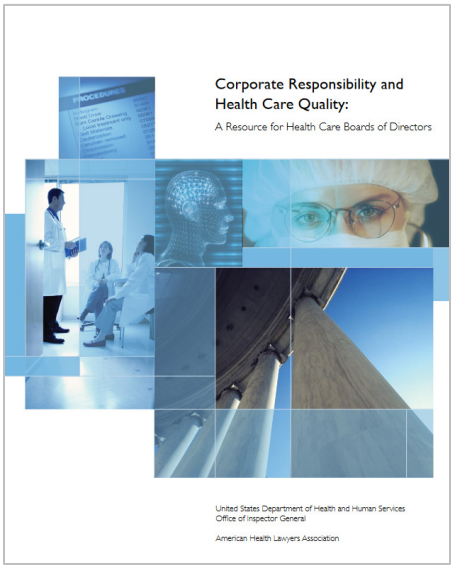
A. Quality and Patient Safety

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

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:

- 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.

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.

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.

SECTION VI
OIG Resources and Processes

Return to TOC

VI. OIG Resources and Processes

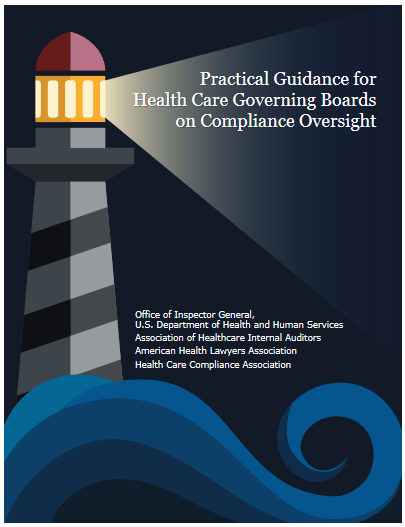
OIG has a Compliance Section on its website that includes numerous compliance and legal resources, such as our CPGs, Advisory Opinions, Special Fraud Alerts, Bulletins, and Other Guidance, Safe Harbor Regulations, Compliance Toolkits, Compliance Resources for Health Care Boards, Provider Compliance Training, 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

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.

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.

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

To submit a question for OIG's consideration as an FAQ, email OIGComplianceSuggestions@oig.hhs.gov.

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.

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.

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.

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.

SECTION VII
Conclusion

Return to TOC

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.

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.