

# HHS-OIG Releases New Compliance Guidance for Healthcare Providers

Insights

11.15.23

This article was published in [Thomson Reuters and Westlaw Today](#) on [November 22, 2023](#).

On November 6, 2023, the Office of Inspector General for the Department of Health & Human Services (the “OIG”) released brand new, updated [General Compliance Program Guidance](#) (“GCPG”) intended as a reference guide for anyone and everyone in the healthcare field, to promote voluntary compliance efforts in preventing fraud, waste, and abuse. Previously, the OIG has issued industry-specific guidance, starting as early as 1998 (for hospitals), and then periodically thereafter, ultimately issuing guidance for home health agencies, laboratories, third-party billing companies, DME, prosthetic, and orthotic suppliers, hospices, Medicare Advantage (MA) plans, skilled nursing facilities, physicians, ambulance providers, and pharmaceutical manufacturers.

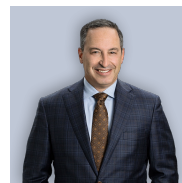
The GCPG is intended to provide general compliance guidance useful for everyone in healthcare. Industry-specific guidance addresses the fraud and abuse risk areas particular to that sector, and the compliance measures that can be undertaken to address those specific risks. For now, the existing industry-specific guidance should be consulted, when applicable to a particular organization. Starting next year, the OIG will be issuing new and updated industry-specific guidance.

The GCPG (and the industry-specific guidance) are not designed to serve as a “model” compliance program, nor are they meant to be “completely comprehensive, or all-inclusive” of every compliance consideration of potential significance. Instead, they are meant to be useful resources, with many practical tips and suggestions for individuals and organizations to use as they see fit in developing their own compliance programs, policies and procedures, as well as hyperlinks to other relevant OIG guidance, statutes and regulations. It is essential to recognize, however, that for all its usefulness, the GCPG (and other OIG guidance) is not necessarily the final word on the laws that the OIG is charged with enforcing; although following the OIG’s guidance can help reduce compliance risks, there is also a range of activity that the OIG has traditionally disfavored that nevertheless remains appropriate and lawful, under certain circumstances.

## I. The Seven Elements

As part of this update, OIG described the seven elements that it considers critical for a successful compliance program. While OIG uses the word “should” in the GCPG, they note that the term is nevertheless intended to present voluntary,

## PROFESSIONAL



**DAVID S. SCHUMACHER**  
Partner  
Boston



**CHARLES B. OPPENHEIM**  
Partner  
Los Angeles  
San Francisco



**BRIDGET A. GORDON**  
Partner  
Los Angeles



**SANDI KRUL**  
Partner  
Los Angeles

nonbinding guidance. At a high-level, those elements are as follows:

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

For each element, the GCPG offers specifics regarding specific items the healthcare compliance community should consider when developing their own compliance programs. A brief summary of some of the key items identified by OIG for each of the seven elements follows.

(1) Written Policies and Procedures

Each organization should have a code of conduct that outlines ethical requirements central to its operations. CEOs and/or boards should endorse and sign the code of conduct to demonstrate organizational commitment. Regular updates to the code of conduct are recommended.

Additionally, each organization should have written compliance policies and procedures, that at the very least encompass (1) the implementation and operation of the entity's compliance program and (2) processes to reduce risks caused by noncompliance with Federal and State laws. It is critical that organizations assess how their specific operations pose compliance risk and ensure there are written policies in place to address those risks. Additionally, policies should be drafted in such a way to foster overall compliance efforts and ensure such policies are updated accordingly. Every relevant individual in the organization should have access to the policies. [\[1\]](#)

(2) Compliance Leadership and Oversight

The organization's board and senior leadership must be committed to compliance, and there should be a compliance officer with the appropriate level of authority to adequately oversee the organization's compliance program and efforts, alongside the assistance of a compliance committee. Compliance officers should have sufficient independence, including not leading or reporting to the entity's legal or financial functions, and not providing the entity with legal or financial advice. A compliance officer may have a dual role as the privacy officer but should be given sufficient staff and resources to perform all tasks associated with such an expanded role.

Organizations should also have a compliance committee with the compliance officer as the chair. The committee should be comprised of relevant leaders of both operational and supporting departments, with adequate information and authority to speak on behalf of their department. New members of the compliance committee should undergo training. Compliance committee meetings should have written meeting minutes and pre-arranged agendas. Additionally, the compliance committee should periodically report to the board and/or executives regarding their performance.

The organization's board also needs to be knowledgeable about the compliance efforts and program at the organization, and the board should oversee the compliance officer and committee and review information provided to assess the organization's compliance risks.

(3) Training and Education

For any successful compliance program, training and education is vital. The compliance officer and compliance committee should develop a training and education approach tailored to the specific risks presented by the organization. Training should cover the entity's compliance program, Federal and State standards applicable to the entity, and board governance and oversight of a health care entity.

Training should be provided at least annually to all board members, officers, employees, contractors, and medical staff (if applicable) of the entity. Additional targeted training should also be developed for specific individuals' roles and responsibilities at the organization, and for board members.

Training materials should be accessible to all required parties, including in all needed languages for diverse employees and contractors. All employees should document participation in training programs and be required to show continued engagement in training as part of their employment.

#### (4) Effective Lines of Communication with the Compliance Officer and Disclosure Programs

All entity personnel should be informed regarding the ways that they can reach the compliance officer directly. Information on these communication options should also be posted in commonly frequented physical and virtual spaces. The organization should also maintain written confidentiality and non-retaliation policies that are distributed to all employees to encourage open communication with the compliance officer and help facilitate reporting of compliance concerns.

The organization should maintain a communication option which allows for anonymous reporting, which should be included in the compliance training. Furthermore, all reports of compliance concerns should be documented in writing, with necessary details regarding the report made (by whom, what date, investigation's findings, corrective action taken, any policy changes, and if any referral was made to state or federal authorities).

#### (5) Enforcing Standards: Consequences and Incentives

The entity's compliance program should establish appropriate consequences for instances of non-compliance, as well as incentives for compliance. The organization should have set procedures for identifying, investigating, and remediating actions that do not comply with the organization's standards, or state or federal law. These procedures should outline the actions that will be taken against employees who engage in improper behavior and should be overseen by the compliance officer to ensure they are applied consistently. Entities should also consider rewarding employees for achieving compliance goals, reducing compliance risk, and/or performing compliance activities outside of an individual employee's job description.

#### (6) Risk Assessment, Auditing, and Monitoring

OIG noted that it has placed an increased emphasis on the importance of a formal compliance risk assessment process for organizations. The process needs to review the risk to the organization stemming from violations of law, regulations, or other legal requirements. Risk assessments should be ongoing and conducted at least annually. The compliance officer and compliance committee should work together to assess risk from external and internal sources, evaluate and prioritize them, and determine which risks need to be addressed. OIG directs organizations to educate themselves on risk assessment methods via a number of specific resources focused on healthcare compliance. It is also recommended that entities use data analytics to understand areas of compliance risk.

Compliance officers and committee also need to continue looking for new and unidentified risks between more formal compliance risk assessments (e.g., legal and regulatory changes, enforcement actions, new entity acquisitions, etc.). The compliance committee should also have a planned schedule for audits to identify risks, including auditing services for their medical necessity. These audits should be designed to periodically assess the compliance program's effectiveness. Reports should be provided to the board regarding the results of assessments of the compliance program's effectiveness.

#### (7) Responding to Detected Offenses and Developing Corrective Action Initiatives

OIG notes that all organizations will at some point receive audit or monitoring results that raise compliance concerns. Otherwise, the lack of anything concerning should raise its own concerns regarding the effectiveness of the entity's compliance program. The compliance program needs to include processes and resources to thoroughly investigate compliance concerns. Furthermore, all such concerns must be reported to the appropriate entity leaders to coordinate with counsel and determine if a violation of applicable law has occurred. Necessary reporting obligations for material violations

must be followed by the organization to the appropriate governmental entity, regardless of whether there was a monetary loss for the government program implicated.

Internal reviews should include taking steps to prevent the destruction of documents or other evidence related to any investigation or audit. Entities should also consider bringing in external counsel, auditors, or health care experts to assist with an investigation. A written record of all investigations should be prepared and maintained by the organization.

If credible evidence of misconduct is discovered, and after a reasonable inquiry, the entity's compliance officer or counsel has reason to believe the conduct may violate criminal, civil, or administrative law, then the entity must promptly make a report to the appropriate governmental entity (not more than 60-days after the determination that credible evidence of a violation exists). OIG emphasized the importance of self-reporting and noted that OIG maintains its voluntary self-disclosure programs for entities to use to report suspected fraud. OIG indicated that it considers the entity's good-faith voluntary disclosure when resolving violations submitted via self-disclosure.

Entities need also take prompt corrective action, including, but not limited to, refunding overpayments (i.e., 60-day report and repay), enforcing disciplinary policies and procedures, and making any policy or procedure changes necessary to prevent a recurrence of the misconduct. Preventing a recurrence will require the organization to identify the root cause of the misconduct and restructure its compliance efforts to prevent that cause prospectively.

## II. Scaling Compliance Programs Based on the Size of the Entity

Just as compliance programs may be structured differently depending on the specific health industry type, the OIG recognizes that compliance programs need to be adapted to fit the size and complexity of the organization. The GCPG identifies various approaches and recommendations to help guide this rightsizing. For example:

*For small entities:*

- If the organization cannot support a compliance officer, it could name a "compliance contact" to manage the entity's compliance activities. This compliance contact should not be responsible for the entity's legal services and, if possible, should not be involved in the entity's billing, coding or claims submission. If there is no corporate board, the compliance contact should report at least quarterly to the owner or CEO on compliance matters.
- Even small entities should have healthcare compliance policies, procedures and training, and the GCPG points to various potential resources to assist in developing those policies, procedures and training materials, including OIG maintained [Compliance Training Videos](#) and its [Roadmap for New Physicians](#).
- Smaller entities might not have formalized disclosure programs, but should have methods and policies in place, suitable for their size and setting, which emphasize the entity's commitment to compliance, require good faith reporting of compliance issues, prohibit retaliation for reporting and help facilitate meaningful and open communication, including, for example, an "open door" policy to raise concerns with the Compliance Contact, owner or CEO.
- No matter the size, the entity should still assess its compliance risks at least once a year and conduct an annual audit. The GCPG refers to certain internet resources to assist with risk assessment, auditing and monitoring, notes that smaller entities can brainstorm during staff meetings to help identify risks and emphasizes the importance of routine monitoring of the List of Excluded Individuals/Entities, state Medicaid exclusion lists and checking practitioners' licensure and certification status. There may also be risk indicators specific to the entity's particular business or practice area that smaller entities may consider for monitoring (e.g., significant changes to number and type of claims rejections, unusual changes in code utilization, etc.).
- There should be enforcement and disciplinary mechanisms in place *before* violations occur, with flexibility to allow for questions and disclosure of mistakes.
- Be prepared to appoint the Compliance Contact or another person to respond to detected offenses and develop steps needed to correct any problems.

*For large entities:*

- It is probably not feasible for a single compliance officer, even if full-time, to successfully implement and maintain an effective compliance program for a large organization. Larger organizations may therefore need multiple compliance personnel, with a chief compliance officer overseeing the program and, depending on the size and nature of the organization, could have deputy compliance officers responsible for specific areas of compliance (e.g., audits, training, policies). The organization's board should have input on the chief compliance officer's appointment, performance evaluation and compensation, and should consider requiring the chief compliance officer to report directly to the board.
- Multi-facility organizations may benefit from regional or facility level compliance officers or liaisons that report (directly or indirectly) to the chief compliance officer. If the facility or location compliance officer is a part-time or secondary role, they should still report directly (or indirectly) to the chief compliance officer on compliance related matters, rather than to the manager of their non-compliance role.
- Larger organizations with compliance committees may consider creating subcommittees under oversight of the larger compliance committee, as well as temporary work groups on certain compliance initiatives.
- Boards should consider creating a separate board compliance committee responsible for overseeing health care compliance (separate and apart from the board audit committee) and, if the chief compliance officer reports to the board, the chain of communication with the chief compliance officer can be delegated to the chair of the board compliance committee or other committee member.
- If the organization is owned or controlled by an international organization, the board of the healthcare organization should ensure that its parent board is sufficiently educated on healthcare laws and compliance risks.

### III. **Other Compliance Considerations**

OIG raised four additional considerations in the new guidance.

First, OIG recommended that health systems incorporate quality and patient safety considerations in compliance programs. While many health care entities treat quality and patient safety as distinct from compliance, OIG noted that there have been a number of published settlements and corporate integrity agreements in recent years involving false claims associated with patient safety and quality of care issues. Thus, OIG recommends that an entity's board of directors and compliance committee receive regular reports regarding quality and patient safety. In addition, the compliance committee should include individuals responsible for quality assurance and patient safety and establish and implement a program to perform quality audits and reviews. And, the compliance officer should incorporate potential quality and patient safety risks into the compliance program.

Second, OIG noted that, in recent years, there have been a number of new entrants into the health care industry, including technology companies, new investors, and organizations providing non-traditional services in health care. OIG is concerned that these new entrants may be unfamiliar with the labyrinth of rules and regulations associated with health care, which prohibit practices that are common in other industries. OIG particularly recommends that new entrants to health care consult the GCPG to assist them in establishing effective compliance programs. Similarly, entities that are branching out into different areas of health care, such as managed care plans or developing new technology, should use the GCPG to guide their compliance efforts in these new ventures.

Third, the OIG reminded the health care community that, in order to operate an effective compliance program, it should "follow the money." In this regard, the OIG highlighted the increased presence of private equity and investment in health care, particularly outside investors providing management services and/or operational oversight with health care entities. In such settings, the OIG recommended that health care entities "carefully scrutinize their operations and incentive structures" to ensure that all activities are compliant with fraud and abuse laws. In addition, the OIG noted that compliance officers must understand the financial incentives associated with any reimbursement system—whether it is fee-for-service or a capitated model—to appropriately tailor a compliance program.

Finally, the OIG recommended that health care entities institute a system to track financial arrangements to ensure that they are compliant, including tracking proper supporting documentation, fair market value assessments, and documenting the business need or rationale for the arrangements.

#### IV. **Take Aways**

With the GCPG, the OIG has set forth benchmark components of an effective compliance program for all health care entities. While the guidance may appear to be daunting—even overwhelming—any health care organization would benefit from thoroughly reviewing the guidance to understand the OIG's expectations. While the guidance is long and detailed, it also includes practical tips and can assist organizations of any size. In any investigation, the OIG or the DOJ scrutinizes the state of compliance at the organization to determine if the potential violation is indicative of a systematic compliance failure or an isolated incident. Even though the guidance is not mandatory, an organization that can demonstrate that it has consulted and internalized key components of the GCPG will be better positioned to avoid the worst outcomes of an investigation, such as large fines or a compliance monitor. By the same token, the OIG is likely to be less sympathetic to organizations that have compliance failures if they have ignored the published guidance.

[1] OIG also recommended that each organization should have a policy and procedure for the screening of all employees, contractors, and other individuals, in particular to check for exclusion from any healthcare programs.

#### **RELATED CAPABILITIES**

[Compliance](#)

[Fraud and Abuse, Stark, Anti-Kickback Counseling and Defense](#)

[Medicare, Medicaid, Other Governmental Reimbursement and Payment](#)

[Hospitals and Health Systems](#)

[Skilled Nursing Facilities \(SNFs\) and Long-Term Care Providers](#)

[Ambulance Providers](#)

[Physicians, Medical Groups, Medical Foundations, and Independent Practice Associations \(IPAs\)](#)

[Drugs and Medical Devices](#)

[Home Health](#)