COSMOS
Navigate the Compliance Universe

Complete Healthcare Compliance Manual
Essential Elements of an Effective Healthcare Compliance Program

By Dr. Cornelia Dorfschmid,[1] PhD, MSIS, PMP, CHC; Debbie Troklus,[2] CCEP-F, CHC-F, CCEP-I, CHPC, CHRC; and Sheryl Vacca,[3] CHC-F, CCEP-F, CCEP-I, CHRC, CHPC

The Office of Inspector General (OIG) offers guidance for healthcare organizations seeking to build effective compliance programs.[4] Their guidance recognizes that there is no one-size-fits-all compliance program. These guidance publications are directed at different segments of the healthcare industry.

Each OIG guidance document outlines seven basic elements that can be tailored to fit the needs and financial realities of any given organization. The OIG believes every effective compliance program begins with a formal commitment to these seven basic elements, which were based on and expanded upon the seven elements described within the Federal Sentencing Guidelines.[5] These seven fundamental elements of an effective compliance program are:

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

The Seven Elements in Practice

The following details how each of the elements can be addressed within a compliance program.

1. Implementing Written Policies, Procedures, and Standards of Conduct

Policies and procedures help set the expectations for all employees and leadership. The Federal Sentencing Guidelines and all OIG program guidance describe this area as one of the seven elements of an effective compliance program. The first of the prescribed elements calls for "the development and distribution of written standards of conduct, as well as written policies and procedures that promote [a healthcare organization's] commitment to compliance."[7] These two types of documents—the standards of conduct (hereinafter referred to as "code of conduct") and the policies and procedures—become the tools used to begin building a compliance program.

The code of conduct is a document that communicates an organization's values and mission and the standards it sets for itself, and serves as an employee resource for how to conduct business at the organization. It demonstrates an organization's ethical attitude and its enterprise-wide emphasis on compliance with all applicable laws and regulations. The code of conduct is meant for all employees and representatives of the organization, not just those most actively involved in compliance issues. This includes third parties (e.g., vendors, suppliers, and independent contractors), which are frequently overlooked.

The code of conduct provides a general road map for proper decision-making—for doing the right thing. It elevates corporate performance in basic business relationships and confirms that the organization upholds and supports proper compliance conduct. The code of conduct is not meant to be a policy but rather a codex of principles (i.e., standards) and can best be understood as the "constitution" of the program. The OIG clearly states that "the code should function in the same fashion as a constitution, *i.e.*, as a foundational document that details the fundamental principles, values, and framework for action within an organization. The code of conduct for a nursing facility should articulate the organization's expectations of employees, as well as summarize the basic legal principles under which the organization must operate. Unlike the more detailed policies and procedures, the code of conduct should be brief, easily readable and cover general principles applicable to all employees."[8]

Whereas a code of conduct provides guidelines for decision-making and behavior, compliance policies and procedures are documents that specifically address identified areas of risk and compliance program operation. Most organizations already have an employee manual that outlines all policies and procedures. Whenever possible, compliance policies and procedures and controls should be integrated into existing policies. And while it is imperative that the organization have policies and procedures, it cannot be emphasized enough that the only thing worse than not having a policy is having a policy and not following it.

Policies and procedures must be living documents that are integral to the day-to-day operation of the organization. That is what the government will question: Are the policies and procedures applied every day? Is someone responsible for the revisions? Are they incorporated into performance reviews and educational programs? Are they reviewed and updated regularly? A code of conduct, policies, and procedures are the essential tools of compliance. But they must be reflective of the actual process and practice to be effective.

Aside from the code of conduct and policies and procedures that describe operations of the compliance program, one type of written guidance is also worth noting: the written charter that defines the responsibility and duties of the compliance committee and, as applicable, a charter of a board committee with responsibility of compliance oversight.

For more information on developing a code of conduct, policies, procedures, and board charter, please see Chapter 3, "Running an Effective Compliance Program."

2. Designating a Compliance Officer and Compliance Committee

The OIG and the Federal Sentencing Guidelines call for the designation of a compliance professional "to serve as the focal point for compliance activities."[9] Whether the position is full time or part time will depend on the size, scope, and resources of the institution. Also, according to the OIG, assigning the compliance officer "appropriate authority is critical to the success of the program."[10] The Federal Sentencing Guidelines state that "to carry out such operational responsibility, such individual(s) shall be given adequate resources, appropriate authority, and direct access to the governing authority or an appropriate subgroup of the governing authority."[11] On a specific level, for example, the compliance officer must have full authority to access any and

all documents that are relevant to compliance activities—documents such as patient records, billing records, contracts with third parties, agents, and any areas of compliance interest. But in the big picture, "appropriate authority" comes from the unquestionable backing of the board of directors or its equivalent, the source of the respect that will get things done.

The compliance officer may be the focal point of a compliance program, but this person cannot be the only focus or assigned all compliance responsibilities. Everyone is responsible for compliance. Compliance-related committees add to the infrastructure of an effective compliance program. The OIG urges a compliance committee be established "to advise the compliance officer and assist in the implementation of the compliance program."[12] Although there is no specific direction about the composition of the committee, the OIG does note that the committee will benefit from having varying perspectives "such as operations, finance, audit, human resources, utilization review, social work, discharge planning, medicine, coding and legal, as well as employees and managers of key operating units."[13] It will serve the organization well to a have a physician representative.

Such a compliance committee is meant to be a management level committee that has all key operational departments represented on the committee. This will be conducive to effective oversight that ensures implementation of annual risk assessments and internal reviews, which are considered a major function of such a committee and are often mandated in corporate integrity agreements (CIAs). Aside from the management-level compliance committees, board-level compliance committees are not uncommon in larger organizations where boards delegate board-level oversight to a special committee.

The board or governing body that sets the tone at the top and vision for the organization's compliance program designates and evaluates the performance of the compliance officer. The management-level compliance committee assists the compliance officer and facilitates integrating compliance controls into operational functions. The compliance officer runs the daily operations of the program. These three functions are the three core components that define the infrastructure of and assigned responsibility for the compliance program.

For more information on the compliance committee, compliance officer role, and board, please see Chapter 3, "Running an Effective Compliance Program."

3. Conducting Effective Training and Education

Education and training are the first and possibly the most important lines of defense for a compliance program. The revised Federal Sentencing Guidelines and all OIG guidance publications identify the need for education and training. The Federal Sentencing Guidelines state that "The organization shall take reasonable steps to communicate periodically and in a practical manner its standards and procedures, and other aspects of the compliance and ethics program…by conducting effective training programs and otherwise disseminating information appropriate to such individuals' respective roles and responsibilities."[14] The OIG's "Compliance Program Guidance for Third-Party Medical Billing Companies" states, "The proper education and training of corporate officers, managers, employees and the continual retraining of current personnel at all levels are significant elements of an effective compliance program."[15]

The OIG suggests training be separated into two types: a general session on compliance for all employees and a second session covering more specific information for appropriate personnel.

General training sessions are meant to heighten awareness among all employees and communicate and emphasize (and then update and reiterate) the organization's commitment to ethical business behavior, which affects all employees. The OIG urges that "all relevant levels of personnel be made part of various educational and training programs" and that "employees should be required to have a minimum number of educational hours per

year, as appropriate, as part of their employment responsibilities."[16] For a frame of reference, a minimum of one to three hours annually for basic training in compliance areas is required in many CIAs.

Specific/focused training in high-risk areas is critical for specialized personnel. Specific or focused education should be provided when there is a new law or regulation, new policy or procedure, or for remedial efforts. The OIG notes, "Clarifying and emphasizing these areas of concern through training and educational programs are particularly relevant to a hospital's marketing and financial personnel, in that the pressure to meet business goals may render these employees vulnerable to engaging in prohibited practices."[17]

The OIG guidance states that, "attendance and participation in training programs be made a condition of continued employment and that failure to comply with training requirements should result in disciplinary action, including possible termination, when such failure is serious. Adherence to the provisions of the compliance program, such as training requirements, should be a factor in the annual evaluation of each employee," and that the organization "should retain adequate records of its training of employees, including attendance logs and material distributed at training sessions."[18]

At the end of general training, employees, as well as volunteers and contracted members of the workforce, should be required to sign and date a statement or produce an attestation that confirms their knowledge of and commitment to the code of conduct. This attestation, according to the OIG, is to be retained in the employee's personnel file. Each organization must decide how ardently to pursue 100% attestation.

For more information on education and training, please see Chapter 3, "Running an Effective Compliance Program."

4. Developing Effective Lines of Communication

There are a variety of methods for employees to report potential problems or to raise concerns. The OIG stresses the importance of communication in the compliance process: "An open line of communication between the compliance officer and…employees is equally important to the successful implementation of a compliance program and the reduction of any potential for fraud, abuse, and waste."[19]

The Federal Sentencing Guidelines also encourages these open lines of communication by stating that an "organization shall take reasonable steps…to have and publicize a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation."[20]

Important to the success of the compliance program is an open-door policy, one where employees feel comfortable approaching supervisors and/or the compliance professional and openly discussing any potential problem. If employees feel comfortable, the chain of command should be followed in discussing issues.

For any reporting method to be effective, employees must accept that there will be no retaliation or retribution for coming forward. The concept of nonretaliation is fundamental to the compliance program, and a clearly stated policy regarding nonretribution for good faith reporting is the first step. It should also be understood that employees have a duty to report any suspected violations of law or compliance policies. To facilitate good faith reporting, confidentiality and the possibility of anonymous reporting are also key. Policies and procedures should assure, to the extent possible, confidentiality and anonymity within legal limits. Training should effectively communicate the commitment to nonretaliation to employees.

Remember, to the government, and in effective compliance, documentation is everything. All complaints must be

logged and tracked and properly maintained. Many organizations assign a unique number to each call or report so that the caller or reporter can check on the status of the complaint by contacting the organization and providing the assigned number. How the complaint was handled, by whom, and when all should be included in the documentation. Documentation of the specifics of the issue, the department(s) involved, findings, and actions taken is important for follow-up so the issues can be closed regardless of the action taken. A clearly stated procedure outlining the disposition of these forms is also needed; specifically, who gets copies and how information is incorporated into written reports. Investigation reporting templates should be discussed by the risk partners before beginning documentation to clarify the preferred format of documentation (e.g., document all interviews or summarize the interviews). Also, discussion should clarify how the finding should be reported (e.g., substantiated with rationale or not substantiated). Finally, it is important for the compliance professional to be clear on who will decide whether or not the investigation supported the findings and who will recommend next steps to management for action.

Reporting works both ways, of course, and the compliance officer should take every opportunity to keep in touch with all levels of staff. Regular ongoing communication and periodic outreach is another form of education that reiterates commitment and can facilitate prevention of problems. Periodic reminders on compliance activities and expectations are useful in this endeavor, too (e.g., newsletters, Compliance Week, email reminders).

For more information on reporting methods, documentation, and communication, please see Chapter 3, "Running an Effective Compliance Program."

5. Conducting Internal Monitoring and Auditing

An effective compliance program is one with a process of constant evaluation. Compliance internal monitoring and auditing is ultimately about managing compliance risks. Auditing and monitoring are basically two types of reviews, where auditing is more rigorous and formal. The key is to strive for and demonstrate a process for continually improving on compliance activities and ensuring that risks are detected, corrected, and prevented from recurring. The OIG's emphasis on the importance of evaluation is evident in that all CIAs call for regular monitoring (at least annually). In numerous recent CIAs, the OIG provided more clarity on what they expect with regard to risk assessments that are part of the auditing and monitoring function of the compliance program. In many recent CIAs, the OIG calls for a centralized annual risk assessment and internal review process to identify and address risks associated with an organization in participation in the federal healthcare programs, including, but not limited to, the risks associated with the submission of claims for items and services furnished to Medicare and Medicaid program beneficiaries.

The compliance committee is considered responsible for implementation and oversight of the risk assessment and internal review process. The risk assessment and internal review process is to (1) identify and prioritize risks, (2) develop internal audit work plans related to the identified risk areas, (3) implement the internal audit work plans, (4) develop corrective action plans in response to the results of any internal audits performed, and (5) track the implementation of the corrective action plans in order to assess the effectiveness of such plans.[21]

Moreover, all OIG compliance program guidance publications state that "an ongoing evaluation process is critical to a successful compliance program."[22] The OIG further explains that "one effective tool to promote and ensure compliance is the performance of regular, periodic compliance audits by internal or external auditors who have expertise in Federal and State health care statutes, regulations and Federal health care program requirements."[23] The OIG calls for audits to focus on programs or divisions, including external relations with third-party contractors, especially those with substantive exposure to government enforcement action.

The Federal Sentencing Guidelines also state that an organization shall take reasonable steps "to ensure that the

organization's compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct."[24]

There are expectations and practices of auditing and monitoring not only for the compliance officer and compliance committee, but also the board. The board should ensure that management and the board have strong processes for identifying risk areas. Risk areas may be identified from internal or external information sources. The board should ensure that management consistently reviews and audits risk areas, as well as develops, implements, and monitors corrective action plans. One of the reasonable steps an organization is expected to take is "monitoring and auditing to detect criminal conduct."[25]

There are at least two ways to approach auditing: the concurrent audit and the retrospective audit. A retrospective audit will provide a baseline assessment of where you are in a period of time in the past, a snapshot, or essentially a laundry list of all the things or errors that occurred and you need to fix.

Concurrent audits are real time, but harder to execute, because the organization must collect all the needed information regarding events occurring in the present versus the past. However, this approach is one of the best ways to effect change. A concurrent audit will identify and address potential problems individually as they arise. If there is indeed an issue, then an organization can correct the related policy or procedure if applicable, communicate the change and then go back in, say, three months and perhaps again in six months, to review and be sure the issue is resolved.

Monitoring is something that is done on a daily or routine basis and does not require independence or standards and protocols as rigorous as audits require. This is a key tool for management to get a sense of their operational controls and help identify potential problem areas. Monitoring is predominantly an operational function and can best be understood as self-policing within operational departments. Compliance may also conduct monitoring to determine whether compliance elements (such as dissemination of standards, training, and disciplinary action) have been satisfied and controls are working. It will also target potential deficiencies and areas where modifications might be in order.

Auditing and monitoring should be documented. At a minimum, a report of findings should be shared with department management, and if activity is part of the overall compliance risk priorities, then the compliance committee, senior leadership, and—where necessary—the board should receive this information. The OIG hospital guidance calls for written evaluations to be presented to the CEO, governing body, and members of the compliance committee no less than annually. The "Program Guidance for Third-Party Medical Billing Companies" adds that when a facility is part of a larger corporate entity, monitoring and auditing activities should be a key feature of any annual review. Appropriate reports on audit findings should be periodically provided and explained to a parent organization's senior staff and officers.[26] Reports to management, the governing body, and the compliance committee should include findings or suspicions of misconduct with recommendations and a management action plan to address and resolve the potential problem.

For more information on risk assessment, please see Chapter 3, "Running an Effective Compliance Program." For more information on auditing and monitoring, please see Chapter 4, "Evaluation Processes, Investigations, and Noncompliance Response."

6. Enforcing Standards Through Well-Publicized Disciplinary Guidelines

"Fair, equitable, and consistent" are the watchwords for enforcing the code of conduct, policies, and procedures. The place to start with enforcement is back at the beginning with the code of conduct, policies, and procedures. The OIG believes that the compliance program should "include a written policy statement setting forth the

degrees of disciplinary actions that may be imposed upon corporate officers, managers, employees, physicians and other health care professionals for failing to comply with the hospital's standards and policies and applicable statutes and regulation," and the organization should " publish and disseminate the range of disciplinary standards for improper conduct and to educate officers and other hospital staff regarding these standards. The consequences of noncompliance should be consistently applied and enforced, in order for the disciplinary policy to have the required deterrent effect. All levels of employees should be subject to the same disciplinary action for the commission of similar offenses."[27]

The Federal Sentencing Guidelines also state that an "organization's compliance and ethics program shall be promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct."[28]

Failure to detect or report an offense is a serious act of noncompliance and equally as deserving of discipline as the actual misconduct. Compliance is an active, ongoing process that is everyone's responsibility. In this area, the compliance officer and staff should work closely with the organization's human resources (HR) department. There are no doubt disciplinary policies and procedures already in place for any disciplinary action. It is HR's responsibility to work with management on imposing discipline. It is the compliance professional's responsibility to monitor consistency in disciplinary actions for fairness and proportionality to offenses.

The OIG calls for the written code of conduct to address the procedures for handling disciplinary problems and those who will be responsible for taking appropriate action. Punishment should be commensurate with the offense. It is important that issues of various levels of seriousness be addressed consistently. There are offenses such as blatant acts of fraud that warrant immediate termination. But most infractions will be relatively minor and most likely unintentional. These may best be handled with education or additional training.

In the context of enforcing standards, the OIG also urges a "new employee policy," which applies particularly to those who have the authority to make decisions regarding compliance issues or supervise those who do. The organization is urged to do "a reasonable and prudent background investigation, including a reference check" as part of the application process.[29] Include a review of the federal healthcare sanctions lists as part of this investigation. Also, the application form itself should ask the job candidate to note any incidents of criminal conviction or exclusion action. This proactive strategy can prevent hiring a sanctioned individual. Such cautions apply to third parties as well. Footnote 48 in the "Compliance Program Guidance for Hospitals" calls for compliance programs to "establish standards prohibiting the execution of contracts with companies that have been recently convicted of a criminal offense related to health care" or which have been determined to be ineligible to participate in federal healthcare programs.[30]

Enforcement is not just about discipline, of course. It is also about incentives. Goals and objectives for individuals and departments can include specific references to compliance. Achievement of those goals, especially when celebrated, is a positive reinforcement that encourages support for and enforcement of the compliance program.

When it comes to enforcement and investigations that lead to enforcement action, the compliance officer may also want to collaborate and coordinate as necessary with legal counsel and internal audit not only to ensure appropriate resources but also to be able to invoke privilege where necessary.

For more information on incentives and discipline, please see Chapter 4, "Evaluation Processes, Investigations, and Noncompliance Response."

7. Responding Promptly to Detected Offenses and Undertaking Corrective Action

If there should ever be reason to believe that misconduct or wrongdoing has occurred, the organization must respond appropriately and in a timely fashion. Failure to respond or to engage in lengthy delay can have serious consequences. The OIG notes that violations of the compliance program and other types of misconduct threaten an organization's status as "a reliable, honest and trustworthy provider capable of participating in Federal health care programs," and that "detected but uncorrected misconduct can seriously endanger the mission, reputation, and legal status" of the organization.[31]

The Federal Sentencing Guidelines state that "after criminal conduct has been detected, the organization shall take reasonable steps to respond appropriately to the criminal conduct and to prevent further similar criminal conduct, including making any necessary modifications to the organization's compliance and ethics program."[32]

Ignoring a legitimate report of wrongdoing will also alienate staff, especially the person who reported the problem, and hence encourage qui tam (whistleblower) action. Cover-ups usually cause more problems than they solve. In the event of misconduct, acknowledge the problem, get the facts, and fix it. However daunting it may feel to be faced with the possibility of misconduct, remember that one of the goals of a compliance program is detection. Having found a problem is an indication the program is working.

The OIG recommends an investigation any time a potential violation is identified. Therefore, a compliance program's plan of action will likely begin with a thorough internal investigation. The internal investigation must be handled with skilled investigators and documented according to the organization's policy. The OIG calls for prompt reporting of misconduct to the appropriate governmental authority within a reasonable period, but not more than 60 days after determining that there is credible evidence of a violation related to payment for services and not more than 30 days to avoid stricter fines. If a repayment is due to Medicare, it must be made within 60 days of identification.[33] The Centers for Medicare & Medicaid Services final rule states that a person has identified an overpayment when the person has, or should have, through the exercise of reasonable diligence, determined that the person has received an overpayment and quantified the amount of the overpayment.[34] Overpayments must be reported and returned only if a person identifies the overpayment within six years of the date the overpayment was received. There may be other time frames applicable to the allegation, depending on the type of misconduct (e.g., Stark, Anti-Kickback, harassment).

If the investigation finds the allegation was not substantiated, no further action is required. However, if after the internal investigation there is reason to believe the organization's misconduct constituted a material violation of civil law or the rules and regulations governing federally funded healthcare programs, then the organization must take steps to disclose the violation to the government.

When reporting to the government, an organization should provide all information relevant to the alleged violation of applicable federal or state law(s) and the potential financial or other impact of the alleged violation. The compliance officer, under advice of counsel and with guidance from the governmental authorities, could be requested to continue to investigate the reported violation. Once the investigation is completed, and especially if the investigation ultimately reveals that criminal, civil, or administrative violations have occurred, the compliance officer should notify the appropriate governmental authority of the outcome of the investigation, including a description of the impact of the alleged violation on the applicable federal healthcare programs or their beneficiaries.[35]

Any identified problem must be corrected quickly and with demonstrably reasonable speed and diligence. Restitution of overpayments especially should be prompt. CMS regulations and contractor guidelines outline procedures for returning overpayments to the government. A provider should consult with its Medicare

contractor for guidance regarding processing Medicare repayments and to establish the information necessary to quantify the amount of the overpayment. And when the problem is rectified, the issue should be added to the list of topics to be addressed with regular internal monitoring. Similar processes should be implemented for Medicaid and other federal healthcare programs to avoid violations of the False Claims Act.

For more information on investigations and corrective action plans, please see Chapter 4, "Evaluation Processes, Investigations, and Noncompliance Response."