COSMOS
Navigate the Compliance Universe

Compliance Today - June 2020
Establishing a best practice approach for your compliance, privacy, and security programs

By Kelly McLendon, RHIA, CHPS

Kelly McLendon (kmclendon@complianceprosolutions.com) is Managing Director at CompliancePro Solutions in Titusville, FL.

Healthcare compliance is based, in large part, on the Department of Health and Human Services (HHS) Office of Inspector General (OIG) model compliance programs,[1] which must be understood and implemented by all compliance officers working in healthcare. For example, the seven elements of a compliance program evaluation are based on Chapter 8 of the U.S. Sentencing Guidelines for Corporations.[2] Each organization must tailor the elements of model compliance programs that are similar to their needs to develop best practices for their compliance efforts. Best practices are a combination of rules, regulations, and the most efficient and effective ways of performing operations, whether manual or automated.[3]

The content published by OIG is presented as a series of voluntary compliance program guidance documents,[4] but they may also be a source of focus by OIG and other regulatory investigators as a part of their enforcement activities. The guidance is directed at various segments of the healthcare industry, such as hospitals, nursing homes, third-party billers, and durable medical equipment suppliers, to encourage the development and use of internal compliance controls to monitor adherence to applicable statutes, regulations, and program requirements.

Since the HHS model compliance programs are quite voluminous and complex, a good place to start is with a discussion of key elements and their best practices. From there, one can progress into increased granularity by illustrating some of the requirements for the specific areas of privacy and security that deal with compliance assessment, which provide guidance about related best practices. The Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security rules[5] call for conducting both privacy and security program assessments to create a best practice standard for how privacy and security compliance is managed.

Seven elements of the OIG model compliance program

The following elements have been identified by OIG as areas of focus for assessment and evaluation of compliance programs.[6] Ensure they are addressed when assessing, measuring, and evaluating compliance program elements.

- "Implementing written policies, procedures and standards of conduct;
- "Designating a compliance officer and compliance committee;
- "Conducting effective training and education;
- "Developing effective lines of communication;
- "Enforcing standards through well-publicized disciplinary guidelines;

- "Conducting internal monitoring and auditing; and
- "Responding promptly to detected offenses and developing corrective action."

Measuring compliance program elements is mandatory under virtually all compliance rules and regulations. In order to facilitate a best practice approach, start with defining expectations of performance or standards for each element. Then, devise assessments or audits to measure and report the results while paying attention to any variances.

For example, a standard for compliance education may be that every senior leader should receive two hours of training annually. If there are 20 senior leaders, and 16 achieved the standard, it's a 75% achievement rate. Report the reasons for the variance within proper governance channels with a year-to-year comparison of results and a plan for remediation. The following year asses it again to determine if the remediation actions have been successful and tweak further if needed.

OIG model compliance program key element best practices

The U.S. Department of Justice guidance titled *Evaluation of Corporate Compliance Programs*[7] offers useful information about how it reviews and assesses compliance programs looking for violations. This guidance is not healthcare-industry specific, but it is illustrative of the elements used for compliance program evaluations. The following items show where the Department of Justice's attention is focused. Compliance program governance must address each of these areas with organized best practices.

- Analysis and remediation of underlying misconduct,
- Conduct of and commitment by senior and middle management,
- Stature of the compliance function,
- Autonomy of the compliance function,
- Compliance program funding and resources,
- Corporate response to expressed compliance concerns,
- Process for responding to findings,
- Disciplinary action consistency,
- Risk management process,
- Frequency of updates to policies and procedures, and
- Whether direct reporting of compliance violations to the board of directors is established and possible.

Compliance governance

An overarching governance structure must be put into place within any organization that has governmental rules and regulations with which they must comply.[8] Typically, governance is managed by senior-level administration, with the required compliance departments and staff size appropriate for the organization's size. It is mandatory to adequately staff company compliance programs—failure to do so is a violation of multiple rules.

One best practice—for organizations that are large enough to warrant it—is having a compliance committee. Membership should be established with senior leaders, including the CEO. The chief compliance officer (CCO) should chair the committee and recognize quorum's requirements. Detailed minutes of the required regularly scheduled meetings should be taken. Meetings should be scheduled monthly or quarterly and occur with established ground rules. Compliance committees should establish a charter that reflects thoughtful development to guide their operations.

All organizations with compliance responsibilities should have an appointed CCO. Typically, these organizations will have multiple compliance efforts to manage the need for a single point of leadership. The CCO has several best practices associated with the role, many of which can be incorporated into the job description. Examples include:

- The CCO should be able to make proper decisions without fear of retaliation.
- *The lead admitter of patients to the hospital is in violation of the medical records completion policy*. The CCO should be able to revoke privileges as policy states.
- *The CEO's spouse is asking to review sensitive and confidential information related to an upcoming community fundraiser*. The CCO should be able to treat her as if she were a normal citizen.
- The CCO should be independent and report directly to the board.

The CCO should be a subject matter expert and have certifications proving their validity, as well as a list of conferences attended, presentations made to industry, etc. However, no one in this business knows everything. It is ok to ask for help. Is the CCO able to get help when it is needed? For example, a CCO may need a subject matter expert in coding and reimbursement issues, which can be notoriously complex. Are they able to get one?