Compliance Today - February 2020

Separating compliance and legal, Part 2: Best practices for an effective compliance program

By Jack A. Rovner

Jack Rovner (jrovner@hlconsultancy.com) is an attorney and the co-founder of Health Law Consultancy, a Chicago-based boutique law firm.

Part 1 of this article (published in the January 2020 issue of*Compliance Today*) explored cautionary tales that illustrate the peril to effective compliance programs of assigning the compliance function to the organization's chief legal officer (CLO), instead of engaging an independent chief compliance and ethics officer (CCEO) as a senior executive in charge of compliance.

Part 2 reviews practical considerations why a compliance function separate and independent from legal is the "best practice" for serving an organization's interests and success. Part 2 examines the federal health industry regulators' views on separating compliance from legal, and explains why cooperation and collaboration between separate, but equal, compliance and legal leadership put an organization on a solid foundation for legal and ethical conduct. Part 2 closes with "Murphy's List" of 10 concrete reasons for keeping compliance separate from legal. The goal is to stimulate organizations in general, and especially those operating in the healthcare sector, to give careful consideration to how best to structure their compliance and legal functions to optimize these critical components of an ethical, successful enterprise.

The government's view—Don't mix hats

The federal government, through the Centers for Medicare & Medicaid Services (CMS), operates the Medicare Advantage (MA) program as an alternative means for Medicare beneficiaries to obtain their Medicare health benefits. To make MA plans available, CMS contracts with private health insurance companies. These insurance companies, called MA organizations, are required by applicable CMS regulations to adopt and implement an effective compliance program. This Medicare regulatory mandate includes designation of "a compliance officer…who report[s] directly and [is] accountable to the organization's chief executive officer or other senior management."[1]

CMS guidance for MA organizations expresses strong preference that the CCEO and compliance function be separate and independent from the CLO and the legal function. CMS's *Medicare Managed Care Manual* specifies that "[t]he compliance officer should be independent [and] not serve in both compliance and operational areas (e.g., where the compliance officer is also the CFO, COO or GC)"; the reason is to avoid "self-policing in the operational area(s)," which can create "conflict of interest."[2]

To be clear, neither CMS regulations nor guidance directs that the mandated CCEO cannot be, or be

subordinate to, an MA organization's CLO. CMS guidance acknowledges that, although an MA organization "must ensure that reports from the compliance officer reach the [organization's] senior-most leaders (typically the CEO or president)," that "direct reporting relationship between the compliance officer and the senior-most leadership refers to the direct reporting of information, not necessarily to a supervisory reporting relationship"; consequently, the required direct reporting "can be accomplished through a dotted line or matrix reporting."[3]

These comments reflect government recognition that "one size won't fit all" and, hence, there is no one "correct" compliance structure. What matters is that the compliance structure adopted and implemented be "effective" and have "measures that prevent, detect, and correct non-compliance with CMS's program requirements, as well as measures that prevent, detect, and correct fraud, waste, and abuse."[4]

Perhaps for smaller or more resource-constrained organizations, combining compliance with legal may be the only practicable solution. But if the organization has the resources, there appears to be a better choice. As CMS sees it, the compliance officer "must have express authority to provide unfiltered, in-person reports to the sponsor's senior-most leader [without first being] routed…through operational management such as the COO, CFO, GC…or other executives responsible for operational areas." To protect that authority, CMS argues that "best practice [will] allow the compliance officer to meet in Executive Session with the [organization's] governing body [i.e., the board]."[5]

CMS's preference for compliance independent from legal has been implemented by the Office of Inspector General (OIG) of the U.S. Department of Health and Human Services. In corporate integrity agreements (CIAs) that resolve federal fraud and abuse and False Claims Act cases, OIG has shown willingness to impose the separation of compliance from legal. In the 2009 CIA with drug-maker Pfizer, which settled (for $2.3 billion) fraud and abuse and False Claims Act charges of illegal off-label prescription drug promotion, OIG required that Pfizer have an executive-level "Chief Compliance Officer [who] shall not be, or be subordinate to, the General Counsel or Chief Financial Officer." The requirement that the "Chief Compliance Officer shall not be, or be subordinate to, the General Counsel or Chief Financial Officer" has generally become the standard for OIG's CIAs.[6]

OIG's chief counsel at the time of the Pfizer CIA explained that this CIA requirement, which removed Pfizer's compliance function from under its general counsel, was "intended to eliminate conflicts of interest, and prevent Pfizer's in-house lawyers from reviewing or editing reports required by" the CIA. The reason for this separation is that "lawyers tell you whether you can do something, and compliance tells you whether you should."[7]

OIG's CIAs also generally mandate that the "Chief Compliance Officer shall be a member of senior management…, shall report directly to the Chief Executive Officer…, shall make periodic (at least quarterly) reports regarding compliance matters directly to the Audit Committee of the Board of Directors…, and shall be authorized to report on such matters to the Audit Committee at any time."[8] The OIG CIAs mandate that the CCEO be "a member of senior management" reporting directly to the CEO and the board, which mirrors CMS guidance for MA organizations that "[i]t is best practice for the compliance officer to be a member of senior management" so that the chief compliance officer can "raise compliance issues without fear of retaliation."[9] No Balla Bind here (for definition, see Part 1 of this article).

Compliance best practice—Collaborating hats

The CCEO and the compliance function should—indeed, must—work in close, constructive collaboration with the CLO and the legal function. That collaboration can enable the CCEO to enlist the investigative aid and tools of the organization's legal function to gather evidence to determine whether there has been a compliance deficiency. The CCEO will then have the facts to decide whether and how to report and remedy the issue.

Separately, the investigative capabilities of the legal function can enable the CLO to advise the organization's senior management and board of directors within the scope of the attorney-client privilege of potential legal liability exposure and the means to manage and mitigate that exposure. Among the benefit of separating the compliance and legal functions is that, when advising management and the board, there should be no ambiguity that the CLO is acting as the organization's attorney providing privileged advice, and not as the organization's CCEO reporting compliance deficiencies and their remediation outside the attorney-client privilege. Put differently, it avoids the Balla Bind and the Sulzbach Parable (see Part 1 of this article) and frees the compliance officer to do the compliance job, secure in legal protection from retaliatory firing.

Murphy's List—Fit the hat to the job

Long-time compliance consultant and attorney Joe Murphy[10] provides a "top ten" list of reasons the CLO ought not also to serve as the CCEO. Joe Murphy presented this list at a meeting of the Chicago Regional Business Ethics Network on February 10, 2009. His list of reasons appears below as numbered subheads. (My explanations for these reasons are provided in plain text; I alone am responsible and accountable for the explanations.)

1. Lawyer as witness

If the CCEO is also the CLO, the company's lawyer may have to become a company witness if the company needs to present the facts about its compliance program, its investigative process of potential compliance failures, or its corrective action. A lawyer usually cannot be both a fact witness and legal counsel for the organization that the lawyer represents. Moreover, lawyer-as-witness usually puts the attorney-client privilege at risk. The CCEO, who is not also acting as corporate attorney, can testify as an organization's fact witness, and doing so would not put the attorney-client privilege at risk.

2. Loss of privilege

If the CCEO is also the CLO, uncertainty about the hat that person wears when investigating and advising on compliance problems could put the attorney-client privilege at risk. Consider the Sulzbach Parable and the Balla Bind—was Sulzbach's direction to Tenet management to fix the physician contracts privileged advice of the CLO or the corrective action of the CCEO? Was Balla's urging not to accept the defective dialyzers privileged legal advice or a nonprivileged compliance directive?

3. Mandatory "Miranda" warning

The CLO investigating compliance problems needs to be upfront in witness interviews of company officers and employees that counsel represents the company, not these individuals. The CLO may even need to caution the officer or employee to obtain the advice of a lawyer who represents the officer or employee. A CCEO faces no such obligation when conducting witness interviews, unless the CCEO is acting under the direction and on behalf of the CLO (a situation in which the CCEO is essentially carrying out a legal function). The reason is a CCEO, not acting for the CLO, provides no basis for an individual officer or employee to assume the CCEO is acting in a legal capacity or represents anyone other than the company.

4. Management skills, not legal skills

Compliance takes management skills—the ability to develop and implement policies, procedures, training, and processes that nurture a "culture of compliance" and persuade officers and employees of the value of ethics and integrity to business success. Compliance is expected to develop and execute programs of audit and oversight to monitor compliance on an ongoing basis. And compliance is ethically bound to act to correct compliance deficiencies. These are skills and roles not generally expected of lawyers. Rather, lawyers are "problem-solvers" and "risk mitigaters" who give advice on how to act within the bounds of the law, rather than taking action themselves. Lawyers are expected to interpret and advise on the law and are not usually expected to be champions for "doing what's right" versus "doing what's legal."

5. Just the usual legal business

Compliance is ethics, culture, and vigilance. Compliance is not just "legal stuff." Compliance is the process of deciding the "right thing" when an issue may be in a legal grey area. The CLO could, within the bounds of legal responsibilities, explain the options for determining when, under applicable FDA regulations, the organization had "sufficient" grounds to require reporting of the Gambro's devices' apparent problems, but a CCEO, getting reports of patient injuries, would be ethically bound to act to get the organization to "do the right thing" and alert the FDA in case immediate remedial action may be required.

6. Ethics, not just law

Compliance is about ethics and ethos—doing the "right thing" because the "right thing to do" is the corporate culture. Compliance reflects a value judgment that ethics and integrity are good business and good for corporate prosperity. Law is about conforming conduct to statutory and regulatory rules. Legal interpretation is about line-drawing between the lawful and unlawful and divining the shades of grey in between. Compliance kicks in where law leaves off. "Law" permitted Morton Thiokol management to decide to approve the Challenger launch; "compliance," in the form of engineering ethics, argued to scrub the launch.

7. Legalistic approaches

Lawyers are called upon to find legal means for accomplishing their clients' objectives. This often requires interpretation of legal niceties and application of law to facts for which established legal standards do not always fit well. Compliance is about keeping an organization on the straight and narrow, sticking to its corporate ethos as captured in its code of ethical business conduct, and doing the "right thing" even when law may appear to allow other choices. When the CCEO is also the CLO, an organization may be sending confusing signals to officers and employees that compliance is just

"legal stuff."

8. More than giving advice

The CCEO is expected to provide an ethical compass for doing "what is right." Compliance operates hotlines/helplines as "safety valves" for corporate officers, employees, and others to anonymously seek ethical guidance and report ethical (if not legal) concerns. Compliance is expected to investigate and to act to remedy divergence from the corporate ethos. The CLO is usually expected to provide legal advice without moralistic overtones. The CLO receiving reports of legal concerns is generally obligated to disclose the reports and the reporters to the client—the company (i.e., senior management or the board)—and usually cannot assure anonymity to reporters. The CLO's duty to the client is one of the reasons that corporate counsel should caution people who report compliance concerns that counsel represents the company and has no obligation of confidentiality to the reporters. The CCEO may want to provide the same caution, and must do so if acting on behalf of the CLO, but otherwise does not face the assertion that the person who reported compliance concerns "believed" the CCEO was acting as the reporter's lawyer who is obligated to maintain the reporter's confidences.

9. Not everyone calls a lawyer

Employees and others may be willing to seek compliance guidance from and disclose compliance concerns to the CCEO—particularly if the corporate code of business ethics assures anonymity. They may be reluctant to share their compliance concerns with the CLO. That's particularly true if they understand or are properly cautioned that the CLO owes a professional duty to the client—the company—to disclose to senior management or the board a reported compliance concern and the reporter of it.

10. More than putting out fires

Legal problems usually involve discrete projects, such as commercial transactions, contract disputes and other controversies, personnel issues, or statutory and regulations construction. Legal issues all too frequently arise as emergencies, if not raging fires, that need to be contained and extinguished. Compliance is much more than firefighting and emergency response. Effective compliance is every day, every way—a continual corporate program of persistent vigilance involving ongoing training, monitoring, oversight, and process improvement.

Conclusion

Their distinctive roles and responsibilities, regulatory mandates, government guidance, and best practice borne of experience—all argue for the CCEO and compliance function to be independent of the CLO and legal function. The need for compliance independence is rooted in avoiding the potential conflict between the CLO's duties of providing privileged legal advice on the organization's legal obligations and potential legal exposures, and the CCEO's duties of implementing and monitoring compliance with the organization's code of ethical business conduct and preventing, detecting, and correcting compliance deficiencies.

Murphy's List, the Sulzbach Parable, the Balla Bind, and the Challenger disaster—each argues for compliance separate from legal and a CCEO separate from the CLO. Assuredly, an organization's

legal and compliance functions must be closely coordinated and work interactively. But their roles and responsibilities differ markedly. Legal is tasked with advising on what the law requires; compliance is tasked with pressing for "what is right." Keeping these very different roles and responsibilities separate enables compliance and legal to perform their distinct functions with integrity and effectiveness—to the best benefit of the organizations they serve.

Takeaways

- Compliance "best practice" separates an organization's compliance function from its legal function.
- Real world cautionary tales tell why—to avoid the inherent conflict between the roles, responsibilities, and expectations of compliance versus legal.
- Compliance serves a public function, favoring transparency in enforcing an organization's pledge of ethical business conduct.
- Legal serves a private function, operating under the obligation to maintain client confidences in protecting the organization's interests within the bounds of the law.
- Compliance and legal must cooperate, coordinate, and complement each other to work in tandem for the best benefit of the organization they serve.

1 42 C.F.R. § 422.503(b)(4)(vi)(B) .
2 CMS, *Medicare Managed Care Manual* (*MMCM*), Pub. 100-16, Ch. 21 § 50.2.1 (January 11, 2013), https://go.cms.gov/2OXuGCM.
3 CMS, *MMCM*, Ch. 21, § 50.2.1.
4 42 C.F.R. § 422.503(b)(4)(vi) .
5 Office of Inspector General, U.S. Dep't of Health & Human Services, Ass'n of Healthcare Internal Auditors, American Health Lawyers Ass'n & Health Care Compliance Ass'n, *Practical Guidance For Health Care Governing Boards On Compliance Oversight* 10 (April 20, 2015), https://bit.ly/2DThYyM.
6 OIG, *Corporate Integrity Agreement between OIG and Pfizer, Inc.* § III.A.1 (Aug. 31, 2009) (hereinafter *Pfizer CIA*).
7 Jim Edwards, "Pfizer's Lawyers Play Musical Chairs in Wake of Bextra Settlement,"*CBS News MoneyWatch*, September 23, 2009, https://cbsn.ws/389KEBf.
8*Pfizer CIA*, *supra* n. § III.A.1.
9 CMS, *MMCM*, *supra* n. 2, Ch. 21 § 50.2.1.
10*See* www.joemurphyccep.com.