

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).

This document is only available to members. Please log in or become a member.

[Become a Member](#) [Login](#)