A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

COMPLIANCE TODAY MAGAZINE

AUGUST 2026

ANDREA EKLUND
SENIOR VICE PRESIDENT, COMPLIANCE & INTERNAL AUDIT, CHIEF COMPLIANCE OFFICER AT BAPTIST HEALTH

COMPLIANCE SHAPES HOW AN ORGANIZATION THINKS, DECIDES, AND OPERATES (P6)

HCCA

COMPLIANCE AS A GOVERNANCE FUNCTION: WHAT BOARDS SHOULD EXPECT FROM THEIR CCO

by Andrew B. Heineman

CCB article click for CEU quiz

Andrew B. Heineman
(aheineman@honesthealth.com, linkedin.com/in/andrewbheineman) is the Chief Compliance Officer at Honest Health in Nashville, TN.

The governance gap continues

At this year's 30th Annual HCCA Compliance Institute, a conversation continued around how best to align boards with their compliance program. Most healthcare boards—depending on the company size and sector within healthcare—have a compliance program. Far fewer have a clear, shared expectation of what the chief compliance officer (CCO) should deliver to the board, in what form, and with what regularity. The relationship between compliance leadership and board oversight exists structurally in almost every organization and is required by multiple government agencies, as will be discussed later. In practice, however, it is often underdeveloped, episodic, and heavily filtered through management layers that reduce rather than enhance the board's ability to exercise meaningful oversight.

This is a governance design problem and one that regulators, governance authorities, and industry leaders have been signaling for years. As compliance professionals, we need to keep pushing until we see sufficient maturity across the healthcare industry.

The U.S. Department of Health and Human Services Office of Inspector General (OIG) has long underscored the board's central role in compliance oversight. In its foundational resource, *Practical Guidance for Health Care Governing Boards on Compliance Oversight* (developed in partnership with HCCA, the American Health Lawyers Association, and the Association of Healthcare Internal Auditors), OIG describes the governing board's compliance oversight role as a core fiduciary obligation—not a function that can be simply delegated.[1] More recently, OIG's *General Compliance Program*

Guidance (*GCPG*) reinforced this expectation, designating "Compliance Leadership and Oversight" as the second of seven elements of an effective compliance program and specifying that boards must be knowledgeable about the compliance program's content and operation and exercise reasonable oversight of its effectiveness.[2]

We see similar expectations from outside the healthcare sector as well. Twice in recent years, the U.S. Department of Justice (DOJ) has provided updates that reinforce the structural needs organizations must meet to ensure effective compliance programs. First, in 2024, DOJ updated their guidance for the *Evaluation of Corporate Compliance Programs*. The update included earlier requirements to ensure the program is well designed, resourced adequately, empowered to function (i.e., structural and actual empowerment), and works in practice, but this time added questions ensuring a focus on emerging technologies, strengthening whistleblower protections, and supporting efforts of the compliance team to access data on the program.[3] Second, in 2026, DOJ released its first-ever Corporate Enforcement Policy, which should push all corporate entities to strengthen internal reporting, identification, and a means to address those concerns.[4]

The National Association of Corporate Directors (NACD) has raised parallel concerns from the governance side. Its 2023 *Board Trends and Priorities Survey* flagged a persistent mismatch between director skills and the top risk issues organizations face, identifying "information flow issues between the board and management" as the second greatest barrier to high board performance.[5] Compliance information flow is a primary driver of that barrier in healthcare organizations, specifically.

The gap between what boards should know about compliance and what they actually receive can be addressed. It requires both sides of the board–CCO relationship to understand their respective responsibilities.

How the CCO role has evolved—and why boards have not kept up

The CCO role in healthcare emerged in the 1990s as a largely reactive function. It was a response to high-profile enforcement actions, the U.S. Sentencing Guidelines, and OIG's early compliance program guidance for hospitals published in 1998.[6] The original framing was primarily defensive: build a program, train your staff, create a hotline, and reduce the organization's exposure to the False Claims Act, the Anti-Kickback Statute, and other federal fraud and abuse laws.

Over the intervening decades, the role has matured considerably. Today's CCO is expected to function as an enterprise risk leader, a culture steward, a regulatory horizon scanner, and a governance partner to organizational frontlines, executive management, and the board—three quite different stakeholders. The *GCPG* reflects this evolution, recommending that large healthcare entities ensure the compliance officer has the "authority, stature, access, and resources necessary to lead an effective compliance program" and that the compliance officer has "independent access" to the board of directors.[7]

The *GCPG* further recommends that healthcare entities consider separate board-level compliance and audit committees, and that board members receive training specifically addressing "board governance and oversight of a health care entity." While the *GCPG* is not written as a set of requirements, it does represent the federal government's expectations for effective board oversight of compliance.

The challenge is that board engagement with compliance has often not kept pace with the CCO role's evolution. Many boards still interact with compliance the way they did 15 years ago: receiving episodic updates during committee meetings, framed primarily around incident reports, regulatory developments, and training completion rates. The CCO presents, the board receives, and the conversation moves on. This information transmission misses the target of governance and oversight.

The CCO presents, the board receives, and the conversation moves on. This information transmission misses the target of governance and oversight.

What effective board–CCO engagement actually looks like

Effective board oversight of compliance is not defined by how much information the board receives

or the quantity of meetings between the board and its CCO. It is defined by the quality of the dialogue between them and information that enables such conversations. The *Practical Guidance for Health Care Governing Boards on Compliance Oversight* offers a practical framework: boards should expect regular reports from compliance, internal audit, legal, HR, quality, and information technology. Pointedly, that information should be received separately and independently to preserve the integrity of each function's voice. OIG specifically recommends using dashboards or scorecards that include key financial, operational, and compliance indicators to help boards assess risk against budget, strategic plan, and policies and procedures.[8]

A well-functioning board–CCO relationship includes the following elements:

- Regular, structured compliance reporting that addresses forward-looking risks—not only historical incidents. The board should be receiving horizon intelligence—not just a rearview mirror.
- Direct access to the audit or risk committee for the CCO, not solely filtered reporting through the CEO or general counsel. The *GCPG specifies that the compliance officer must have this access, and boards should protect it.*[9]
- A shared framework for what compliance program effectiveness means at the board level. This includes agreed-upon indicators that allow the board to assess program effectiveness—not simply activity.
- CCO participation in board-level strategic risk conversations, particularly when new business lines, acquisitions, technology implementations, or payment model changes are under consideration.
- Regular executive sessions between the board and compliance, legal, audit, and quality leadership—conducted without management present—to preserve the board's ability to receive an unfiltered perspective.

The Delaware courts established the foundational legal standard in the 1996 *Caremark* decision: Corporate boards have a fiduciary duty of care that requires ensuring information and reporting systems exist that are "reasonably designed to provide to senior management and to the board itself timely, accurate information" to allow informed judgments about the organization's compliance with the law.[10] For healthcare boards, this duty is operationalized through the board's relationship with the CCO. A board that has not designed that relationship to meet the *Caremark* standard is not mitigating their governance risk.

The questions every board should ask its CCO

OIG has long encouraged boards to be active, questioning, and appropriately skeptical in their oversight role. They should "raise questions, and exercise some degree of skepticism" rather than serve as passive recipients of management-curated information.[11]

The following questions are examples of the kind of inquiry that distinguishes effective compliance governance from compliance theater:

- What are the top three compliance risks you are monitoring that are not yet on the board's agenda? This question highlights the gap between what management manages and what the board oversees.
- How would you describe the current state of our compliance culture, and what evidence supports that assessment? Culture is the leading indicator of compliance program effectiveness. Boards that only track program activity miss the more predictive signal.
- If a federal regulator conducted an unannounced review tomorrow, where would we be most exposed? This question tests the CCO's candor and the board's tolerance for honest assessment.
- What does our compliance program currently lack that would make it more effective? A CCO who cannot answer this question is either not engaged or not empowered.
- *How are we incorporating quality and patient safety into our compliance program? The* GCPG *recommends integrating quality and patient safety into compliance program oversight and board reporting.*[12]
- How is our compliance program adapting to emerging risk areas, including AI, cybersecurity, and new payment models? NACD data shows approximately 40% of companies now charge at least one board-level committee with AI oversight responsibilities, nearly four times the share that did so in 2024. Healthcare compliance programs need to be ahead of this shift: built in, not bolted on afterward.
- What information are you not getting from management that would help you do your job? This question, asked directly to the CCO, is one of the most important governance acts a board can perform.

What the CCO should proactively bring to the board

The board–CCO relationship is not a one-way flow of information. Effective compliance governance requires that the CCO proactively deliver the information boards need to exercise meaningful oversight—without waiting to be asked. A CCO functioning as a true governance partner should bring the board:

- Synthesized risk intelligence, not raw compliance data. Boards need interpretation, not volume. The compliance report that runs 40 slides has often communicated less than the one that runs four, with a clear assessment of where the organization stands and where it is exposed.
- Culture indicators, including hotline utilization trends, retaliation concerns, tone-at-the-middle assessments, and findings from compliance training effectiveness monitoring. These are the leading indicators that precede enforcement exposure.
- Regulatory and legislative horizon scanning. The CCO should be the board's early warning system for changes in enforcement priorities, new OIG guidance, and emerging risk areas in the healthcare regulatory environment.
- Program effectiveness data, including results of internal audits, monitoring activities, and corrective action outcomes. The *GCPG* identifies risk assessment, auditing, and monitoring as a core element of any effective compliance program.
- Quality and patient safety integration. As OIG has made clear, compliance programs that operate in isolation from quality and patient safety functions miss a critical dimension of organizational risk and board oversight responsibility.

A CCO who waits to be asked questions is leaving governance value on the table and potentially exposing your board. The fiduciary standard requires that the board have the information it needs to exercise informed oversight. Boards expect CCOs to be the experts in their domain and bring appropriate materials and information to them. Meeting this standard is a shared responsibility between the board and the compliance function.

Implications for how boards structure compliance oversight

The governance architecture around compliance in most healthcare organizations has not kept pace with the compliance function's expanded scope. Several structural changes over the years merit serious consideration, and this need is only becoming more pressing as enabling technologies accelerate the pace of business.

First, boards should assess whether their current committee structure gives compliance oversight sufficient dedicated attention. The *GCPG* specifically recommends that large healthcare organizations consider separate board-level compliance and audit committees, but there is similar value to having these committees in smaller organizations. Board-level compliance committees should be composed of members most knowledgeable about the business's regulatory risks. They can then focus on the data and details of risks instead of summaries, which are more likely to reach the entire board.

Additionally, when structured with appropriate authority, these committees can authorize actions and, with fewer calendars to coordinate amongst, should result in quicker activity. The full board still retains responsibility, but there are operational benefits to adopting OIG's committee suggestion. The scope of the committee matters as well. The NACD has noted that as AI adoption accelerates and risk complexity grows, audit committees—which currently endure the most compliance, legal, cybersecurity, and now AI risk at most organizations—may need structural relief.

A CCO who waits to be asked questions is leaving governance value on the table and potentially exposing your board.

Second, boards should evaluate whether their current directors possess the compliance and governance fluency necessary to fulfill the oversight role OIG and federal courts expect. The U.S. Sentencing Guidelines require that an organization's governing authority be knowledgeable about the content and operation of its compliance and ethics program and exercise reasonable oversight of its effectiveness. This is a knowledge standard, not merely a structural one. Board composition

should reflect it, but this has been a longstanding gap for many boards, even here in the healthcare space. CCOs should raise this as a risk to their boards; industry organizations (i.e., HCCA, SCCE) should continue to push for this board experience; and we are likely to see this requirement identified in government findings and settlements.

Third, boards should formalize their expectations of the CCO function through a board-approved compliance oversight charter or equivalent governance document that specifies reporting frequency, content requirements, escalation thresholds, and the CCO's direct access to board leadership. The absence of such a document is a governance gap.

OIG has been clear that compliance program governance is not a one-size-fits-all obligation, but it has been equally clear that boards bear meaningful responsibility for ensuring their compliance oversight efforts are genuine—not performative. The standard is "meaningful effort," and what constitutes meaningful effort is calibrated to each organization's size, complexity, and risk profile.[13]

A different kind of compliance leadership

The compliance leaders who will be most valuable to healthcare organizations in the next decade are those who have helped our industry mature beyond simply mastering regulatory impacts. It is no longer enough to simply move beyond the "department of no" stigma. The most valuable compliance leaders will be those who understand that governance is a lever and see compliance not as a set of obligations to be satisfied but as an infrastructure of institutional trust to be built and sustained. That infrastructure serves the board and, ultimately, the patients whose healthcare organizations aim to impact. It gives board directors the information they need to exercise the oversight the law requires and their duties demand. It enables confident decision-making in uncertain times. It holds up under regulatory scrutiny. And it protects the organization, its patients, and its people from the consequences of preventable governance failures.

Healthcare boards should not simply ask whether their entity has a compliance program as a check-the-box exercise; they should ask if they have a board–CCO relationship that makes the compliance program governable. That relationship does not exist simply by having a CCO. It has to be designed, maintained, engaged, supported, challenged, and taken seriously by all parties.

Boards that get this right reduce their compliance and legal exposure for certain. But they also result in structures that are harder to compromise and more capable of delivering on their mission while supporting their organization's value propositions. CT

Endnotes

1. U.S. Department of Health and Human Services, Office of Inspector General, Association of Healthcare Internal Auditors, American Health Lawyers Association, and Health Care Compliance Association, *Practical Guidance for Health Care Governing Boards on Compliance Oversight, April 20, 2015*, https://oig.hhs.gov/documents/root/162/Practical-Guidance-for-Health-Care-Boards-on-Compliance-Oversight.pdf.
2. U.S. Department of Health and Human Services, Office of Inspector General, *General Compliance Program Guidance, November 6, 2023,* https://oig.hhs.gov/documents/compliance-guidance/1135/HHS-OIG-GCPG-2023.pdf.
3. U.S. Department of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs, September 2024,* https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl?inline.
4. U.S. Department of Justice, Criminal Division, *Corporate Enforcement and Voluntary Self-Disclosure Policy, March 2026,* https://www.justice.gov/dag/media/1430731/dl?inline.
5. Reid Sawyer, *A Call to Action: Elevate Board Risk Oversight, NACD Directorship Special Issue 2024: The Future of the American Board, National Association of Corporate Directors, January 22, 2024,* https://www.nacdonline.org/all-governance/governance-resources/directorship-magazine/2024-future-board-special-issue/a-call-to-action-elevate-board-risk-oversight/.
6. U.S. Sent'g Guidelines Manual, § 8B2.1 (U.S. Sent'g Comm'n 2025), https://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2025/GLMFull.pdf.
7. Office of Inspector General, U.S. Department of Health and Human Services, *General Compliance Program Guidance, 37.*
8. *Practical Guidance for Health Care Governing Boards on Compliance Oversight, 12–13.*
9. Office of Inspector General, U.S. Department of Health and Human Services, *General Compliance Program Guidance, 37–38.*
10. In re Caremark Intern. Inc. Deriv. Lit., 698 A.2d 959, 970 (Del. Ch. 1996), https://law.justia.com/cases/delaware/court-of-chancery/1996/13670-3.html.
11. Gregory Demske, "Guidance for Health Care Boards," U.S. Department of Health and Human Services, Office of Inspector General, podcast, March 27, 2013, https://oig.hhs.gov/newsroom/oig-podcasts/guidance-health-care-boards/.
12. Office of Inspector General, U.S. Department of Health and Human Services, *General Compliance Program Guidance, 76.*
13. *Practical Guidance for Health Care Governing Boards on Compliance Oversight, 6.*

Takeaways

- **Evolve oversight expectations**: The chief compliance officer's (CCO) role has matured from reactive defender to strategic governance partner. Boards must update their engagement to match this enterprise risk leadership.
- **Deliver synthesized intelligence**: CCOs must provide synthesized risk assessments, culture indicators, and horizon scanning rather than raw data or historical incident reports to enable true board oversight.
- **Ensure structural independence**: Boards must guarantee the CCO direct, unfiltered access to leadership, including regular executive sessions—without management present—to preserve objective reporting.
- **Ask probing questions**: Boards must abandon passive listening. Directors should ask direct questions about emerging risks, compliance culture, and unmitigated exposures to fulfill their fiduciary duties.
- **Upgrade committee structure**: To handle growing regulatory complexity, organizations should establish dedicated, board-level compliance committees staffed by directors with deep regulatory and governance fluency.