2018 HEALTHCARE COMPLIANCE OUTLOOK FOR BOARDS OF DIRECTORS

BY JAYNE E. JUVAN & KELLI R. NOVAK

With the 2016 election of Donald Trump, some healthcare industry experts predicted a substantially relaxed enforcement environment. Fatigued by burdensome regulation under the Obama Administration, many welcomed change. However, now that Trump's first year has come to a close, it is clear that the fight against healthcare fraud has not completely fallen by the wayside. We may one day look back and conclude that enforcement under the current administration was indeed less aggressive; still, the level of activity in the administration's first year underscores that boards of directors of healthcare organizations must remain vigilant in their compliance efforts to ensure that the organizations they serve do not end up in the government's crosshairs.

THE BOARD'S ROLE IN HEALTHCARE COMPLIANCE

The U.S. Department of Health and Human Services, Office of Inspector General (OIG) consistently advises boards of healthcare organizations of the importance of fulfilling their oversight responsibilities. In *Practical Guidance for Health Care Governing Boards on Compliance Oversight*, an article co-published by OIG, OIG indicated that boards need to be fully engaged in carrying out this role.

Delaware law is considered to be the gold standard in articulating corporate governance standards, as it is the most sophisticated in defining director fiduciary duties — in part, because of the high number of corporations incorporated there. When issuing healthcare guidance, OIG has similarly cited Delaware law in analyzing a board's oversight responsibilities under state law and has expressed a need for boards to understand these state law duties.

Under Delaware law, directors have a fiduciary duty of care and loyalty. The duty of care provides that the board has a responsibility to act with the care an ordinarily prudent person in a like position would exercise under similar circumstances. Pursuant to the duty of loyalty, the director shall perform duties in good faith and in a manner the director reasonably believes to be in, or not opposed to, the corporation's best interests.

Because courts prefer not to second-guess business decisions, boards enjoy "business judgment rule" protection — a judicially-created presumption that, in making a business decision, the directors acted on an informed basis, in good faith, and in the honest belief that the action taken was in the best interest of the corporation. In a court action, a plaintiff must demonstrate that the director breached the duty of care or loyalty to rebut the presumption.

In *In re Caremark International, Inc. Derivative Litigation*, the court indicated that the duty of care encompasses a board's duty to monitor. Pursuant to *Caremark*, an "utter failure to attempt to assure a reasonable information and reporting system exists" or a conscious failure to monitor such a system after it is implemented would constitute a breach of the duty of care. In *Stone v. Ritter*, the court tied this analysis to the duty of loyalty, saying that the duty of good faith is a subsidiary element of the duty of loyalty, and it is a breach of the duty of good faith to intentionally fail to act in the face of a known duty to act. The conditions for liability are (i) "utterly failing to implement any reporting or information controls" or (ii) "consciously failing to monitor… thus disabling themselves from being informed."

In *Practical Guidance*, OIG illustrates its view of the applicability of this analysis to healthcare organizations. Citing *Caremark*, OIG states, "[a] Board must act in good faith in the exercise of its oversight responsibility for its organization, including making inquiries to ensure: (1) a corporate information and reporting system exists and (2) the reporting system is adequate to assure the Board that appropriate information relating to compliance with applicable laws will come to its attention timely and as a matter of course."

OIG emphasizes that boards should adopt corporate compliance programs to ensure the organization is and remains in compliance with applicable laws and evaluates and responds to illegal activities that occur within it. In structuring these programs, boards may consider documents such as the Federal Sentencing Guidelines, as well as OIG's voluntary compliance program guidance and prior corporate integrity agreements (CIAs). In *Practical Guidance*, OIG states, "Boards are expected to put forth a meaningful effort to review the adequacy of existing compliance systems and functions," making it clear that the responsibility for compliance oversight lies firmly with the board itself and recommending that boards adopt corporate programs to ensure compliance.

One of the most important aspects of a well-designed and implemented corporate compliance program is that, in accordance with the Federal Sentencing Guidelines and OIG guidance, such programs may serve as a mitigating factor if misconduct is detected. Properly implemented compliance programs that include an information reporting system and board oversight may also help a board fulfill its fiduciary duties.

In overseeing the compliance function, boards also should ensure they stay abreast of developments in healthcare laws. Requesting regular updates from the organization's compliance officer, privacy and security officer, or experienced staff results in a better-informed board, placing it in a stronger position when interacting with management.

Listed below are key risk areas boards should be apprised of as they navigate the changing operating environment in 2018 and oversee their organizations' compliance efforts.

KEY RISK AREAS

1. Fraud and Abuse

During the Trump Administration, federal government agency enforcement actions have continued, and there are attempts to strengthen efforts with a proposed $70 million funding increase for the Health Care Fraud and Abuse Control Program.

Recent fraud investigations shed new light on motivations contributing to the opioid crisis — a target of the current administration. The Department of Justice reported that 2017 marked the largest takedown in U.S. history, involving over 400 practitioners responsible for $1.3 billion in false billings from prescribing and distributing opioids and other narcotics. At the corporate level, opioid sales practices and incentives are being closely scrutinized.

Companies in specific service lines deemed at high risk for fraud and abuse are also on OIG's radar. OIG's 2017 Work Plan targets home-based and community-based services, ambulance transportation, durable medical equipment, and diagnostic radiology and laboratory testing.

2. Corporate Integrity Agreements

With the continued focus on fraud and abuse, it is no surprise that 2017 revealed a rise in CIAs. Last year, OIG entered into 52 CIAs — exceeding the five-year annual average of 43 CIAs. The 52 CIAs demonstrate increasing penetration into the healthcare industry including laboratories, hospices, pharmacies, specialty medical practices, EMS, and home care. Significantly, some CIAs named corporate officers as parties, in addition to the corporate entity itself.

CIAs impose penalties for misconduct that carry significant organizational burdens. Further, a breach of the CIA itself is grounds for additional sanctions — ranging from monetary fines to exclusion from participation in federal healthcare programs.

3. Cybersecurity and Patient Privacy

A May 2017 Executive Order announced cybersecurity as another priority, focusing initially on securing federal networks and enhancing critical infrastructure; however, we anticipate an increase in the breadth of data security regulation — especially in the healthcare industry, recently plagued by data breaches and settlements. In 2017, Anthem paid a record-setting $115 million to settle litigation involving a data breach implicating 80 million customers' personal information.

In response to cybersecurity threats, the Office of Civil Rights (OCR) began publishing more guidance for entities regulated by the Health Insurance Portability and Accountability Act (HIPAA). In June 2017, OCR issued a cyber-attack "Quick Response Checklist," including a four-step response plan to a cyber-related security incident involving a covered entity (CE) or business associate (BA). OCR also publishes monthly "Cyber Awareness Newsletters" on its website. The surge in publically available information creates an expectation that HIPAA-regulated entities be educated and prepared to guard against cybersecurity threats.

Last fall, OCR announced preliminary desk audit results from HIPAA's Phase 2 Audit Program. CEs and BAs located in the Midwest were the highest audit subjects in the country, and early ratings indicate CEs' overall inadequate compliance with HIPAA Privacy, Security, and Breach Notification standards. As of September, BA desk audits were still underway, and we expect on-site audits will follow, which will comprehensively evaluate privacy and security practices of CEs and BAs.

4. Contractual Relationships

Corporations engage countless subcontractors and vendors to perform essential business functions. In the healthcare industry, these engagements must be executed and structured properly to ensure compliance.

Recent six- and seven-figure settlements demonstrate the importance of BA agreements among HIPAA-regulated entities. This includes both executing written agreements and vetting and updating existing agreements to ensure continued compliance. BA agreements are particularly ripe for compliance enforcement in light of OCR's ongoing auditing processes.

Given that a corporation is prohibited from contracting with individuals or entities excluded from federal healthcare programs, its due diligence process and documentation is also subject to scrutiny. Because a party's circumstances can change in an instant and jeopardize a once-appropriate business relationship, a corporation should establish screening processes to regularly monitor their vendors' participation status in federal healthcare programs.

5. Workplace Issues

Healthcare organizations continue to face high employee turnover rates, especially in the skilled workforce. Those who depart may be disgruntled and pose compliance risk. Recent False Claims Act judgments and settlements — up to $331 million — underscore that anyone can become a whistleblower and create exposure to significant monetary and reputational damages. Therefore, building a "culture of compliance" within every level of an organization is of the utmost importance.

Conclusion

Boards of healthcare organizations should closely examine governing laws and ensure that their organizations' corporate and HIPAA compliance programs and other policies and procedures are regularly updated. Periodically participating in training and education on these issues, ensuring that corporate compliance is a recurring agenda item, and making sure that regulatory developments and material compliance incidents are promptly brought to their attention will go a long way in combatting risks.

Jayne E. Juvan is a Partner, Corporate Governance Group co-chair, and Private Equity Group chair at Tucker Ellis LLP. She has been a CMBA member since 2017. She can be reached at (216) 592-5000 or jayne.juvan@tuckerellis.com.

Kelli R. Novak is an Associate at Tucker Ellis LLP, where she serves as a member of the Healthcare Practice Group. She has been a CMBA member since 2013. She can be reached at (216) 592-5000 or kelli.novak@tuckerellis.com.