Murphy’s Law holds that in any complex system, what can go wrong will go wrong. Engineers commonly apply this cautionary principle to the design of systems that must anticipate the unexpected and deliver consistent, reliable performance. But it can also apply to the challenges facing trustees of health care organizations who are trying to comply with increasingly complex and frequently changing regulatory standards. Board members have a fiduciary responsibility to oversee an organization’s operations, including its compliance with legal requirements. In the corporate arena, directors have generally been expected to ensure that:

“Information and reporting systems exist in the organization that are reasonably designed to provide to senior management and to the board itself timely, accurate information sufficient to allow management and the board, each within its scope, to reach informed judgments concerning both the corporation’s compliance with law and its business operations.” [In re Caremark International Inc. Derivative Litigation, 698 A. 2d 959, 970 (Del. Ch. 1996).]
The obligations of trustees of not-for-profit organizations differ somewhat from state to state but also generally demand a prudent level of supervision. Chapter 8 of the 2009 Federal Sentencing Guidelines Manual, which is applicable to all organizations, similarly expects that:

“An organization’s governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program.” [§8B2.1(b)(2)(A) (Nov. 2009)].

Courts have traditionally been reluctant to hold board members personally accountable for an organization’s regulatory failures absent evidence of bad faith or self-dealing. This recognizes the public benefit of encouraging qualified persons to serve on corporate and not-for-profit boards as well as the dangers of second-guessing board actions when circumstances, for unanticipated reasons, have turned out badly. However, the New York State Office of the Medicaid Inspector General recently announced an intention to inquire into board actions:

“…In assuring that compliance processes and systems are in place, and whether board members have exercised reasonable oversight over information and reporting systems. In appropriate circumstances, OMIG will consider sanctions, including censure and/or exclusion against individual members of the governing body for significant failures to comply with their duties with respect to compliance and oversight.” [OMIG 2009-10 Medicaid Work Plan.]

While it is too soon to know whether other jurisdictions will follow New York’s lead, board members in other states would be prudent to consider the level and scope of their own oversight efforts.

Fortunately, there are a number of publicly available resources to assist board members in this regard. The Office of Inspector General for the Department of Health & Human Services has published compliance guidelines for a number of health care sectors. It has also joined the American Health Lawyers Association in producing several white papers designed to help health care trustees understand and fulfill their obligations for effective oversight.

Nevertheless, even where a health care organization has invested in a robust internal regulatory compliance program, board members—particularly those without significant health care regulatory experience—may find it difficult to evaluate its effectiveness. They may be unable to confidently answer questions such as:

• Is the program focusing on the most significant regulatory risks?
• Are internal controls and audit processes reliably identifying and avoiding potential regulatory failures before they can cause material adverse consequences?
• Are significant regulatory failures being promptly reported to senior management and to the board?

Board members who want to enhance their ability to exercise informed and independent oversight of their organization’s compliance programs and protect both the organization and themselves should evaluate their organization’s program using the following yardstick.

1 GOVERNANCE AND RESOURCES. Most organizations have assigned responsibility for regulatory compliance to a designated compliance officer or to the general counsel. Whether the compliance officer role requires a full-time position and what role the general counsel should play in managing or overseeing a compliance program will depend on the size, complexity and management structure of an organization.

Large organizations with the resources to attract and compensate persons to fill separate positions may choose a different approach from organizations that lack these resources. In either case, the board should be able to identify a specific member of senior management with accountability for compliance program design and effectiveness. That person should be qualified to perform the function and have access to sufficient resources to do so effectively. An experienced health care auditor should also be part of the team.

The board itself should assign specific oversight responsibility for regulatory compliance to the audit committee or a separate compliance committee. Committee members should be independent of management and be prepared to commit adequate attention to the subject. Where this would be a challenge for members who are not familiar with health care regulation, the board should consider recruiting at least one trustee with sufficient training and experience to qualify as the regulatory equivalent of the “financial expert” found on many audit committees. Committee members should document their oversight activities and ensure that significant findings and recommendations are reported to the full board.

2 RISK IDENTIFICATION. In recent years, many health care organizations have adopted broad-based enterprise risk management programs. These often include regulatory risk. Board members should ask management to identify the top eight to 10 regulatory risks facing the organization and explain how they are addressed through an ERM or related regulatory compliance program. The scope of the risk pool should not be limited to traditional coding and referral source issues, but should include emerging HIPAA privacy and security issues as well as health care quality. These issues are becoming a focus of increasing enforcement activity and should be part of any comprehensive regulatory risk management program.

Management should be asked to prioritize risks based on the potential harm to the organization as well as the relative likelihood that a regulatory failure could occur. In many cases, the key risks for an organization are likely to be similar to those of other orga-
nizations in the same health care sector, and benchmarking information may be available through government or industry sources. Boards should pay special attention to areas in which the organization has encountered past difficulties, such as poor audit results, government investigations or similar red flags.

Board members should also consider requesting an independent expert to review the thoroughness of risk identification and the reasonableness of risk prioritization. Such a person or firm should be familiar with key regulatory and enforcement trends affecting the organization and should be able to suggest or validate suitable risk and performance benchmarks. The scope and cost of such a review should be tailored to the size and risk profile of the organization.

Board members should not be reluctant to use their own professional experience—as well as common sense—to probe management and any outside experts about potential gaps or weakness in the risk assessment. In particular, they should ask questions about emerging risk areas such as new service lines being initiated by the organization or changes in government regulatory policies or enforcement strategies. For example, a hospital’s internal controls may effectively address regulatory risks associated with inpatient services, but may not be adequate for a line of outpatient services proposed to be offered through a new hospital-based clinic. Keeping pace with an organization’s evolving regulatory risks is an important part of exercising effective oversight of a compliance program.

**INTERNAL CONTROLS.** Once the scope and prioritization of key regulatory risks have been established, board members should seek reasonable assurance that internal controls have been developed to mitigate the highest priority risks. These may include controls designed to prevent regulatory failures from occurring in the first place as well as those designed to detect failures in a timely manner and thereby limit the potential for adverse consequences. Calibrating the cost and efficacy of controls will normally require a thoughtful discussion of risk tolerance among members of the board and management, each recognizing the impossibility of eliminating all compliance risks. No matter how strong their commitment to regulatory compliance, board members and management must ultimately decide how best to allocate inevitably finite resources to achieve a level of risk reduction that is both reasonable and consistent with achieving the organization’s overriding health care mission.

Setting specific performance targets for key regulatory risks will necessarily guide the development of internal controls. For example, a coding accuracy target could be set as a percentage of net payments. This could be linked to Medicare program averages or some other benchmark but adjusted periodically based on experience. Where feasible, the organization should set targets for other common regulatory risk areas including referral source relationships, privacy and quality of care.

Board review and approval of annual compliance plans and budgets will institutionalize this process and ensure available resources are focused on developing or strengthening controls for an organization’s highest priority regulatory risks.

**CONTROL EFFECTIVENESS.** Board members are expected not only to ensure that an internal compliance program is in place, but also to exercise prudent oversight of its effectiveness. This requires timely access to information about compliance program performance and especially about any material program failures. Management should develop appropriate audit tools and other reporting metrics to enable board members to assess whether the program is functioning as effectively as intended (that is, that internal controls are making a measurable difference in mitigating key regulatory risks).

Board members should meet regularly with an organization’s compliance officer, general counsel and auditor to review significant audit reports and other performance data. Results should be benchmarked to targets set by the board, to the organization’s own past history, or to the performance of other organizations in the same health care sector. This should enable board members to evaluate compliance program performance on par with other core organizational functions (for example, sales and expense control) and lay the foundation for more effective management accountability.

Trustees should also pay attention to how management responds to compliance failures. A compliance program that fails to identify any overpayments or other regulatory issues through audit or internal reporting mechanisms is cause for suspicion. Health care regulation has become too complex for everything to work perfectly all of the time. Board members should pay close attention to management’s explanation of how a failure occurred, changes to internal processes or controls, the steps taken to identify and hold accountable those responsible for the failure, and whether the failure requires disclosure to regulatory authorities or repayment of funds to third parties.

**EXTERNAL REGULATORY ISSUES AND TRENDS.** Effective compliance program oversight cannot be entirely inward looking. Because regulatory risks tend to evolve over time, board members should make an effort to stay in touch with significant emerging regulatory risks and challenges. Too often, organizations and board members have been caught off guard by government investigations of regulatory issues that were not adequately understood by management or board members or addressed through effective internal controls. Board members who wish to prevent this from occurring in their own organizations can ask the compliance officer or general counsel to arrange periodic briefings on new regulatory developments or to forward copies of important articles or reports on regulatory topics of particular interest to an organization. Briefings on current inves-
tigations and settlements affecting other providers offering similar items or services may also be helpful. The board should use this process to anticipate new trends and developments likely to affect the organization and to take prudent steps to mitigate potential regulatory vulnerabilities.

**Better Odds**

Ultimately, an effective regulatory compliance program must support—not interfere with—an organization’s central health care mission, which is to address the health care needs of its patients. The accuracy of back office coding and the terms of physician compensation arrangements are important, but clearly secondary to a hospital or health system’s core medical mission. Still, a coding failure or overgenerous compensation arrangement that leads to a multimillion dollar settlement or other repayment can be a drain on financial and management resources that might otherwise be devoted to improving the quality and safety of patient care. It is the board’s responsibility to set the tone for adopting prudent regulatory controls without compromising the organization’s ability to deliver care. Formal compliance plans and frequent communication between the board and management can help maintain this balance and encourage the cost-effective use of resources to meet compliance performance goals.

This kind of strategic collaboration goes to the heart of each board member’s oversight responsibility. Playing an active oversight role in the design, execution and ongoing assessment of an organization’s regulatory compliance program can substantially reduce the likelihood of a material program failure. When Murphy’s Law produces the inevitable system failure, thoughtful and well-documented internal controls may limit the scope of the failure as well as offer protection for both the organization and board members for the consequences of missteps that occur despite good faith efforts to prevent them.

This article is based on a presentation made by the authors at the American Health Lawyers Association Hospitals and Health Systems Law Institute in February 2010.

JOHN MARKUS (jmarkus@balch.com) is an attorney with Balch & Bingham LLP in Birmingham, Ala. He has served as chief compliance officer for several large health care companies following high-profile government enforcement actions, most recently at HealthSouth. JOLEE HANCOCK BOLLINGER is general counsel to Franciscan Missionaries of Our Lady Health System in Baton Rouge, La.