206:HIPAA, HIPAA, Hooray! So You're Compliant, but What Now?

The Honorable Alex M. Azar II
General Counsel
United States Department of Health and Human Services

Leslie C. Bender
General Counsel and Chief Privacy Officer
The ROI Companies

Sarena Straus
General Counsel
MDx Medical Management, Inc.

Faculty Biographies

The Honorable Alex M. Azar II

Alex Azar has served as the general counsel of the United States Department of Health and Human Services since his senate confirmation in August 2001. Mr. Azar supervises an office of 400 attorneys representing a department with over 300 programs and a 2004 budget of over $537 billion, the largest budget of any cabinet department. He and his attorneys have played a key role in the public health response to 9/11 and the subsequent anthrax attacks, the formulation of the Bioterrorism Prevention Act of 2001, the procurement of bioterrorism countermeasures, and the smallpox vaccination program. During his tenure, they have also been involved in medical liability reform, the faith-based initiative, welfare reform, Medicare and Medicaid reform, efforts to reduce the number of uninsured and speed up the availability of generic drugs, the FDA's initiative to encourage science-based nutrition claims, and Secretary Thompson's regulatory reform agenda. In January of this year, Mr. Azar personally defended before the U.S. Court of Appeals for the Fourth Circuit the HIPAA rule protecting the privacy of medical records.

Mr. Azar clerked for Justice Antonin Scalia on the Supreme Court of the United States and served as an associate independent counsel during the first two years of the Whitewater investigation under judge Kenneth Starr. Most recently, he was a partner at Washington's Wiley, Rein & Fielding.

Mr. Azar is a graduate of Dartmouth College and Yale Law School.

Leslie C. Bender

Leslie C. Bender is principal in her own law firm and director of HIPAA services for roiWebEd Company, and specializes in transactional and compliance work primarily for health care clients. Ms. Bender is nationally recognized speaker on various HIPAA and general privacy compliance topics. She consults independently and through roiWebEd with health care organizations and their business associates on HIPAA educational and implementation projects. Ms. Bender has authored numerous articles for national circulation on compliance, HIPAA, and privacy corporate compliance topics.

Prior to these positions, Ms. Bender held a political appointment and executive position in Baltimore's economic development program as part of its federally designated Empowerment Zone. Prior to her Empowerment Zone appointment, Ms. Bender had spent nine years practicing at Washington, DC law firms representing banks and other financial institutions in mergers and acquisitions, loan portfolio securitizations, loan workouts and restructurings, and related compliance and transactional matters. She spent five years as in-house counsel and a vice president and regional manager for what is now Bank of America, N.A.

Ms. Bender is a member of the American Collectors' Association's Members' Attorneys Program, now serving on the MAP Committee (its governing body), ACCA, the American Health Lawyers Association, the International Privacy Officers Association, the WEDi-SNIP National Vendor Education Workgroup, MAHI Central (the regional WEDi-SNIP unit), and has been a frequent speaker over the past 19 years on topics related to HIPAA, credit, collections, privacy, developing and implementing corporate compliance policies, commercial law, and economic and urban development. In July, 2002, as a result of Ms. Bender's contributions to HIPAA educational

programming and government relations work on privacy matters with HHS and the FTC, ACA International awarded Ms. Bender its highest distinction, international Member of the Year.

Ms. Bender received her BA from Northwestern University and her JD from the University of Notre Dame Law School.

Sarena Straus

Sarena Straus is general counsel for MDx Medical Management Inc. in White Plains, New York. MDx has approximately 160 employees and does billing, collections, front end staffing, and HIPAA compliance for over 100 doctors and at several hospitals. Ms. Straus manages all legal issues for MDx including contract negotiations, intellectual property and trademark, litigation, arbitration, subpoenas, real estate and landlord/tenant, medical malpractice, and insurance claims. Ms. Straus also supervises meetings of board of directors and quality assurance committees and ensures compliance with Safe Harbor, STARK, Anti-kickback, HIPAA, and other state and federal regulations.

Prior to joining MDx, Ms. Straus worked at a plaintiffs products liability firm in New York City. She also prosecuted domestic violence, sex crimes, and crimes against children at the Office of the Bronx District Attorney where she specialized in protecting children online. Ms. Straus was featured in a documentary called *Crime and Justice: The Bronx* which aired on the Discovery Channel. Ms. Straus also served as counsel for an internet start-up company called Figleaves.com that specialized in the on-line sale of intimate apparel.

Ms. Straus currently serves as pro bono counsel to The Hudson Valley Center for Contemporary Art in Peekskill, New York. She remains very active in issues pertaining to missing and exploited children. Ms. Straus is a soprano with the New York Choral Society and a published poet. She received her BA from Barnard College and is a graduate of Fordham University School of Law.

HIPAA Reality: Putting HIPAA Into Perspective

American Corporate Counsel Association
October, 2003
Leslie Bender-The ROI Companies
Sarena Straus-MDx Medical Management Inc.

Current Events

- Despite the 24 months health care organizations had to come into compliance with HIPAA's Privacy Rule, misunderstandings are abundant.
- In a survey conducted by Phoenix and HIMSS, nearly a fourth of all health care organizations readily admitted that they were not even minimally compliant preferring to take a "wait and see" approach

More misunderstandings …

- Health care providers are refusing to release medical records to other care giving providers, stating an express patient consent is required first
- Hospitals are refusing to list comatose or other incapacitated patients' names in their facility directories -- thus barring family members from even knowing if their loved ones are in the hospital
- Hospitals are refusing to release facility information to members of the clergy about patients unless the clergy ask for the patient by name
- Clergy are refusing to tell congregations about sick members thinking they must be HIPAA complaint
- Doctors are refusing to discuss patient cases with each other, even in training institutions, because the hospital is telling them it's a HIPAA violation

In other national HIPAA news…

- On April 15, 2003, DHHS released interim enforcement rules and has established an "on line" means for filing privacy complaints
- CMS, a division of DHHS, released the final Security Regulations with an April, 2005 compliance deadline
- A number of organizations are coming out with voluntary HIPAA "certification" programs – URAC, NCQA

From the nation's capitol …

The Health Privacy Project, a Georgetown University based consumer privacy think tank, established a web-based complaint filing Health Privacy Monitoring Program

Closer to home …

Pharmacies are refusing to allow family members to pick up other family members' prescriptions. According to a Walgreens pharmacist, "Close family members, including spouses, won't be able to pick up medical information about the patient, including information about prescriptions, without written permission."

In Congress…

- **July 30, 2003 National Health Information Infrastructure Act of 2003 Introduced in Congress**: The bill, HR 2915 would create within the Department of Health and Human Services (HHS) a national health information officer serving for five years unless Congress extends the term. The officer, in consultation with an advisory group comprised of health care industry members, would issue recommendations for a uniform health information system to ensure compatibility and interoperability. The legislation would also require the development of national, voluntary data and communications standards such as medical vocabularies and electronic messaging.

In the courts….

- **June 3, 2003 Ruling Upholds Patient's Privacy**: The Wisconsin State Court of Appeals upheld a jury's verdict that an EMT invaded a patient's privacy by telling someone else about the patient's overdose. Telling just one person can be enough to invade someone's privacy, the District II appeals panel ruled.
- **May 1, 2003 Suit**: **Hospice Violated Privacy** The lawsuit alleges that the Hospice of the Florida Suncoast violated state law by intentionally releasing medical and personal information about thousands of patients and their next of kin. The suit claims the hospice released the patient information over the last several years as its for-profit subsidiary, Hospice Systems Inc., marketed a software product to other hospices around the nation. The Hospice allegedly used patient information to help demonstrate, market, sell and train people to use the software, also putting some of the information on the Internet.

From the police blotter…

- **May 19, 2003 Murder-Suicide Suspect's Medical Condition Kept Private Under HIPAA**: In what appeared to have been an attempted murder-suicide, Ron Newman, 67, was in critical condition after he was taken to St. Patrick Hospital but hospital officials were unable to release any information about his condition. Invoking HIPAA, his family requested that all medical information remain private. The County Sheriff said he was working with the county attorney's office to determine if there is a legal way to require the hospital to provide Newman's medical condition to either a law enforcement officer or the Deputy County Attorney.

What do we mean by privacy compliance?

- Our privacy compliance is in essence the basis upon which we can responsibly represent that we have adequate safeguards in place to protect both the confidentiality and the integrity of the consumer information (non-public) entrusted to our care.
- But haven't we always been in the business of doing that?

Why privacy compliance?

- Any business charged with handling consumer's financial or medical information must maintain consumers' trust in the integrity of what it does
- As Karen Trudel of the Department of Health and Human Services stated in May, 2003 – "We should comply with HIPAA because it is the right thing to do if consumers entrust their personal information to our care, not because we fear litigation."

Results of poor privacy compliance

- Attrition
- Lawsuits
- An ugly, emotional story in our local paper or on a local news show
- Industry wide concern over privacy leads to heightened public pressure on both courts and legislatures to do something to fix the problem and restore public trust

Results of misunderstanding HIPAA

- Decreased quality of medical care and training
- Difficulty in obtaining records, medicals and information by family members, even for incapacitated patients
- Atmosphere of paranoia rather than at atmosphere of privacy
- Angry patients and doctors

The Federal Trade Commission Act

- 15 USC Sections 41-58
- Under FTC Act, Congress granted the FTC broad authority to prevent unfair methods of competition and **unfair or deceptive trade practices** in or affecting commerce.

The FTC's powers to prevent and redress unfair and deceptive trade practices

Congress granted broad powers to the FTC under the FTC Act. They including the following:

- Prevent or punish companies for unfair or deceptive trade practices – monetary or other relief
- Using its rulemaking powers to define what unfair or deceptive trade practices are
- Report on and recommend legislation
- Conduct investigations

Change in Regulatory Focus

- Previous FTC enforcement focused on activities likely to harm consumers in the collection of their information
- Under the Bush Administration, the FTC's focus is on misuse of consumers' information
  - Notably: identity theft

Heightened Congressional and State Legislative Interest in Privacy Problems as Deceptive Trade Practices

- Bills pending in both the House and Senate to potentially increase FTC's authority regarding various unfair or deceptive uses of consumer's information and to address the collection (and privacy) of patient safety information
- States being pressured by consumer and other advocacy groups to pass more legislation preventing unfair or deceptive uses of consumers' information

HIPAA spreads to non-healthcare related information

- While the US Congress focuses on fighting spam email, legislation aimed at protecting consumer privacy online has taken a back seat. One privacy bill, Sen. Dianne Feinstein's (D-CA) "Notification of Risk to Personal Data Act," which would require companies to notify consumers when a database containing private information has been compromised, might not win passage because of technology industry opposition. A bill that may have more support than Feinstein's is the Consumer Privacy Protection Act of 2003, introduced by Rep. Cliff Stearns (R-FK) and 22 co-sponsors. The Stearns bill requires that companies collecting personal information give customers privacy notices and tell them why the information is being collected.

Today's Situation

- The FTC has an increased focus on enforcing laws with particular emphasis on privacy
- Attorney generals of the states also have the ability to pursue unfair or deceptive trade practices actions under state consumer protection oriented laws
- Private litigants – individuals bringing lawsuits in state or federal courts – trend toward adding unfair or deceptive trade practice to lawsuits

Where is all this heightened enforcement heading?

- Clear indication that organizations entrusted with the care of non-public information of consumers must have responsible policies, practices and operations for assuring that information is not vulnerable to misuse or improper disclosure
- In spite of claims of no private right of action in HIPAA, in California, consumer attorneys are now advertising for consumers who suffered breaches of their medical privacy

Privacy Problems as Unfair or Deceptive Trade Practices

Under Section 5 of the Federal Trade Commission Act, the FTC has determined that even accidental or unintentional breaches of consumers' privacy will constitute unfair or deceptive trade practices.

Are you or your clients at risk for committing deceptive trade practices – how private are you?

- Review your organization's existing policies and procedures governing the use, disclosure and protection of consumer's financial, health or other potentially "non-public" information
- Know what federal and state laws apply to you and your operations and what they say about protecting this non-public information

Features of a privacy compliance program

- Accountability
- Clear and understandable policies and procedures
- Continuous improvement
- Document what you've done and how you've made compliance decisions
- Consumer permission mechanism (what does this mean?)
- Training and education
- Use / Disclosure Controls and logging of all violations
- Sanctions
- Complaint process
- No retaliation or intimidation
- No waiver
- Safeguards – adequate administrative, technical and physical means to safeguard consumer information

Is your workforce operating from a mindset of "awareness"?

- What might happen if a client / customer were to walk through your operations area and ask any member of your workforce about your organization's rules about consumers' information?
- What are your verification procedures on inbound calls?
- How to you identify and react to consumers' requests for information?
- Who is allowed to respond to third party requests for consumers' information?
- Do you have a consumer complaints process?

Testing for general awareness and operations in sync with good privacy practices

- How can you use consumer's information?
- What rules limit or control information you can access?
- What would you tell someone who asks what your privacy policies are?
- How are you supposed to respond to third parties' requests for information and who responds?
- Who in your office is permitted to "release" consumers' information?
- When and where are you supposed to discuss consumer's information?
- What should you do if a co-worker seems to be misusing information? Is it documented?
- Who handles complaints from consumers or internal complaints?
- Do you ever handle the information of VIPs or people you know?
- How does your HR department avoid conflicts?

Recommendations

- Assess whether or not your operations are in sync with privacy laws
- Appreciate that your workforce wants to do the right thing. Is the guidance you give adequate?
- Redesign your policies and procedures to establish clear sanctions for committing such conduct and enforce them
- Take time to properly train and educate your workforce
- Consider whether or not there are marketing opportunities based on your updated customer care approach

Just when you thought you mastered HIPAA's definition…

PHI – that information covered by HIPAA's privacy rule – regardless of form, manner of transmission, etc……

ePHI

- Now the final Security Regulations bring us the concept of "ePHI" - or electronic PHI
- Because the proposed Security Regulations only addressed PHI in electronic form, whether at rest (stored) or in transit (during an electronic transmission) - the final Security Regulations only cover this
- DHHS has, however, reserved the right to come back and issue regulations regarding the other forms of PHI

Data Interchange Issues

- What if any business risks do I have if *am not* as HIPAA compliant from a security perspective as my covered entity clients or other trading partners? What if they are not HIPAA compliant?
- What should I be tracking now?
  - As part of my privacy compliance, do I have the functionality to track all disclosures and generate reports?
  - Can I audit the accounts or other consumer information individuals in my organization access?

Encryption, interoperable systems?

- What electronic means might you be using to communicate consumer information with your clients? How secure does it need to be?
- What "security incidents" do you currently report? Will there be a compliance issue here for you when the Security compliance deadline arrives?

A word or two about business associate agreements….

Land mine clauses to look out for:

- Onerous indemnity provisions
- Injunctive relief or other equitable relief provisions
- Limitations of liability on consumer information transferred
- Strict limitations on the use / disclosure of consumer information – which limitations may be considerably stricter than those in HIPAA itself and which may hamstring you
- Signing agreements you have not read or agreeing to things you lack the ability to do

Thank you for your time.

- Feel free to write me with any questions you may have:
- LCB@theROI.com
- SStraus@mdx-med.com

CORPORATE RESPONSIBILITY AND CORPORATE COMPLIANCE:

A Resource for Health Care Boards of Directors

THE OFFICE OF INSPECTOR GENERAL OF THE U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

AND

THE AMERICAN HEALTH LAWYERS ASSOCIATION

ACKNOWLEDGEMENT

This educational resource represents a unique collaboration between the American Health Lawyers Association and the Office of the Inspector General of the United States Department of Health and Human Services. This publication would have not been possible without the dedicated effort of numerous individuals at both organizations. It is intended to be a useful resource for those serving on the Boards of Directors of our nation's health care institutions.

I. INTRODUCTION

As corporate responsibility issues fill the headlines, corporate directors are coming under greater scrutiny. The Sarbanes-Oxley Act, state legislation, agency pronouncements, court cases and scholarly writings offer a myriad of rules, regulations, prohibitions, and interpretations in this area. While all Boards of Directors must address these issues, directors of health care organizations also have important responsibilities that need to be met relating to corporate compliance requirements unique to the health care industry. The expansion of health care regulatory enforcement and compliance activities and the heightened attention being given to the responsibilities of corporate directors are critically important to all health care organizations. In this context, enhanced oversight of corporate compliance programs is widely viewed as consistent with and essential to ongoing federal and state corporate responsibility initiatives.

Our complex health care system needs dedicated and knowledgeable directors at the helm of both for-profit and non-profit corporations. This educational resource, co-sponsored by the Office of Inspector General (OIG) of the U.S. Department of Health and Human Services and the American Health Lawyers Association, the leading health law educational organization, seeks to assist directors of health care organizations in carrying out their important oversight responsibilities in the current challenging health care environment. Improving the knowledge base and effectiveness of those serving on health care organization boards will help to achieve the important goal of continuously improving the U.S. health care system.

Fiduciary Responsibilites

The fiduciary duties of directors reflect the expectation of corporate stakeholders regarding oversight of corporate affairs. The basic fiduciary duty of care principle, which requires a director to act in good faith with the care an ordinarily prudent person would exercise under similar circumstances, is being tested in the current corporate climate. Personal liability for directors, including removal, civil damages, and tax liability, as well as damage to reputation, appears not so far from reality as once widely believed. Accordingly, a basic understanding of the director's fiduciary obligations and how the duty of care may be exercised in overseeing the company's compliance systems has become essential.

Embedded within the duty of care is the concept of reasonable inquiry. In other words, directors should make inquiries to management to obtain information necessary to satisfy their duty of care. Although in the *Caremark* case, also discussed later in this educational resource, the court found that the Caremark board did not breach its fiduciary duty, the court's opinion also stated the following: "[A] director's obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the Board concludes is adequate, exists, and that failure to do so under some circumstances, may, in theory at least, render a director liable for losses caused by non-compliance with applicable legal standards." Clearly, the organization may be at risk and directors, under extreme circumstances, also may be at risk if they fail to reasonably oversee the organization's compliance program or act as mere passive recipients of information.

On the other hand, courts traditionally have been loath to second-guess Boards of Directors that have followed a careful and thoughtful process in their deliberations, even where ultimate outcomes for the corporation have been negative. Similarly, courts have consistently upheld the distinction between the duties of Boards of Directors and the duties of management. The responsibility of directors is to provide oversight, not manage day-to-day affairs. It is the process the Board follows in establishing that it had access to sufficient information and that it has asked appropriate questions that is most critical to meeting its duty of care.

Purpose of this Document

This educational resource is designed to help health care organization directors ask knowledgeable and appropriate questions related to health care corporate compliance. These questions are not intended to set forth any specific standard of care. Rather, this resource will help corporate directors to establish, and affirmatively demonstrate, that they have followed a reasonable compliance oversight process.

Of course, the circumstances of each organization differ and application of the duty of care and consequent reasonable inquiry will need to be tailored to each specific set of facts and circumstances. However, compliance with the fraud and abuse laws and other federal and state regulatory laws applicable to health care organizations is essential for the lawful behavior and corporate success of such organizations. While these laws can be complex, effective compliance is an asset for both the organization and the health care delivery system. It is hoped that this educational resource is useful to health care organization directors in exercising their oversight responsibilities and supports their ongoing efforts to promote effective corporate compliance.

II. Duty of Care

Of the principal fiduciary obligations/duties owed by directors to their corporations, the one duty specifically implicated by corporate compliance programs is the *duty of care.*[1]

As the name implies, the *duty of care* refers to the obligation of corporate directors to exercise the proper amount of care in their decision-making process. State statutes that create the duty of care and court cases that interpret it usually are identical for both for-profit and non-profit corporations.

In most states, duty of care involves determining whether the directors acted (1) in "good faith," (2) with that level of care that an ordinarily prudent person would exercise in like circumstances, and (3) in a manner that they reasonably believe is in the best interest of the corporation. In analyzing whether directors have complied with this duty, it is necessary to address each of these elements separately.

The "good faith" analysis usually focuses upon whether the matter or transaction at hand involves any improper financial benefit to an individual, and/or whether any intent exists to take advantage of the corporation (a corollary to the duty of loyalty). The "reasonable inquiry" test asks whether the directors conducted the appropriate level of due diligence to allow them to make an informed decision. In other words, directors must be aware of what is going on about them in the corporate business and must in appropriate circumstances make such reasonable inquiry, as would an ordinarily prudent person under similar circumstances. And, finally, directors are obligated to act in a manner that they reasonably believe to be in the best interests of the corporation. This normally relates to the directors' state of mind with respect to the issues at hand.

In considering directors' fiduciary obligations, it is important to recognize that the appropriate standard of care is not "perfection." Directors are *not* required to know everything about a topic they are asked to consider. They may, where justified, rely on the advice of management and of outside advisors.

Furthermore, many courts apply the "business judgment rule" to determine whether a director's duty of care has been met with respect to corporate decisions. The rule provides, in essence, that a director will not be held liable for a decision made in good faith, where the director is disinterested, reasonably informed under the circumstances, and rationally believes the decision to be in the best interest of the corporation.

Director obligations with respect to the duty of care arise in two distinct contexts:

- The *decision-making function*: The application of duty of care principles to a specific decision or a particular board action; and
- The *oversight function*: The application of duty of care principles with respect to the general activity of the board in overseeing the day-to-day business operations of the corporation; *i.e.*, the exercise of reasonable care to assure that corporate executives carry out their management responsibilities and comply with the law.

Directors' obligations with respect to corporate compliance programs arise within the context of that oversight function. The leading case in this area, viewed as applicable to all health care organizations, provides that a director has two principal obligations with respect to the oversight function. A director has a duty to attempt in good faith to assure that (1) a corporate information and reporting system exists, and (2) this reporting system is adequate to assure the board that appropriate information as to compliance with applicable laws will come to its attention in a timely manner as a matter of ordinary operations.[2] In *Caremark,* the court addressed the circumstances in which corporate directors may be held liable for breach of the duty of care by failing to adequately supervise corporate employees whose misconduct caused the corporation to violate the law.

In its opinion, the *Caremark* court observed that the level of detail that is appropriate for such an information system is a matter of business judgment. The court also acknowledged that no rationally designed information and reporting system will remove the possibility that the corporation will violate applicable laws or otherwise fail to identify corporate acts potentially inconsistent with relevant law.

Under these circumstances, a director's failure to reasonably oversee the implementation of a compliance program may put the organization at risk and, under extraordinary circumstances, expose individual directors to personal liability for losses caused by the corporate non-

1 The other two core fiduciary duty principals are the duty of loyalty and the duty of obedience to purpose.

2 *In re Caremark International Inc. Derivative Litigation,* 698 A.2d 959 (Del. Ch. 1996). A shareholder sued the Board of Directors of Caremark for breach of the fiduciary duty of care. The lawsuit followed a multi-million dollar civil settlement and criminal plea relating to the payment of kickbacks to physicians and improper billing to federal health care programs.

compliance.[3] Of course, crucial to the oversight function is the fundamental principle that a director is entitled to rely, in good faith, on officers and employees as well as corporate professional experts/advisors in whom the director believes such confidence is merited. A director, however, may be viewed as not acting in good faith if he/she is aware of facts suggesting that such reliance is unwarranted.

In addition, the duty of care test involving reasonable inquiry has not been interpreted to require the director to exercise "proactive vigilance" or to "ferret out" corporate wrongdoing absent a particular warning or a "red flag." Rather, the duty to make reasonable inquiry increases when "suspicions are aroused or *should be aroused;"* that is, when the director is presented with extraordinary facts or circumstances of a material nature (*e.g.,* indications of financial improprieties, self-dealing, or fraud) or a major governmental investigation. Absent the presence of suspicious conduct or events, directors are entitled to rely on the senior leadership team in the performance of its duties. Directors are not otherwise obligated to anticipate future problems of the corporation.

Thus, in exercising his/her duty of care, the director is obligated to exercise general supervision and control with respect to corporate officers. However, once presented (through the compliance program or otherwise) with information that causes (or should cause) concerns to be aroused, the director is then obligated to make further inquiry until such time as his/her concerns are satisfactorily addressed and favorably resolved. Thus, while the corporate director is not expected to serve as a compliance officer, he/she is expected to oversee senior management's operation of the compliance program.

III. The Unique Challenges of Health Care Organization Directors

The health care industry operates in a heavily regulated environment with a variety of identifiable risk areas. An effective compliance program helps mitigate those risks. In addition to the challenges associated with patient care, health care providers are subject to voluminous and sometimes complex sets of rules governing the coverage and reimbursement of medical services. Because federal and state-sponsored health care programs play such a significant role in paying for health care, material non-compliance with these rules can present substantial risks to the health care provider. In addition to recoupment of improper payments, the Medicare, Medicaid and other government health care programs can impose a range of sanctions against health care businesses that engage in fraudulent practices.

Particularly given the current "corporate responsibility" environment, health care organization directors should be concerned with the manner in which they carry out their duty to oversee corporate compliance programs. Depending upon the nature of the corporation, there are a variety of parties that might in extreme circumstances seek to hold corporate directors personally liable for allegedly breaching the duty of oversight with respect to corporate compliance. With respect to for-profit corporations, the most likely individuals to bring a case against the directors are corporate shareholders in a derivative suit, or to a limited degree, a regulatory agency such as the Securities and Exchange Commission. With respect to non-profit corporations, the most likely person to initiate such action is the state attorney general, who may seek equitable relief against the director (*e.g.,* removal) or damages. It is also possible (depending upon state law) that a dissenting director, or the corporate member, could assert a derivative-type action against the directors allegedly responsible for the "inattention," seeking removal or damages.

Over the last decade, the risks associated with non-compliance have grown dramatically. The government has dedicated substantial resources, including the addition of criminal investigators and prosecutors, to respond to health care fraud and abuse. In addition to government investigators and auditors, private whistleblowers play an important role in identifying allegedly fraudulent billing schemes and other abusive practices. Health care providers can be found liable for submitting claims for reimbursement in reckless disregard or deliberate ignorance of the truth, as well as for intentional fraud. Because the False Claims Act authorizes the imposition of damages of up to three times the amount of the fraud and civil monetary penalties of $11,000 per false claim, record level fines and penalties have been imposed against individuals and health care organizations that have violated the law.

In addition to criminal and civil monetary penalties, health care providers that are found to have defrauded the federal health care programs may be excluded from participation in these programs. The effect of an exclusion can be profound because those excluded will not

3 Law is not static, and different states will have different legal developments and standards. Standards may also vary depending on whether an entity is for profit or non-profit. Boards of public health care entities may have additional statutory obligations and should be aware of state and federal statutory requirements applicable to them.

receive payment under Medicare, Medicaid or other federal health care programs for items or services provided to program beneficiaries. The authorities of the OIG provide for mandatory exclusion for a minimum of five years for a conviction with respect to the delivery of a health care item or service. The presence of aggravating circumstances in a case can lead to a lengthier period of exclusion. Of perhaps equal concern to board members, the OIG also has the discretion to exclude providers for certain conduct even absent a criminal conviction. Such conduct includes participation in a fraud scheme, the payment or receipt of kickbacks, and failing to provide services of a quality that meets professionally recognized standards. In lieu of imposing exclusion in these instances, the OIG may require an organization to implement a comprehensive compliance program, requiring independent audits, OIG oversight and annual reporting requirements, commonly referred to as a Corporate Integrity Agreement.

IV. The Development of Compliance Programs

In light of the substantial adverse consequences that may befall an organization that has been found to have committed health care fraud, the health care industry has embraced efforts to improve compliance with federal and state health care program requirements. As a result, many health care providers have developed active compliance programs tailored to their particular circumstances. A recent survey by the Health Care Compliance Association, for example, has found that in just three years, health care organizations with active compliance programs have grown from 55 percent in 1999 to 87 percent in 2002. In support of these efforts, the OIG has developed a series of provider-specific compliance guidances. These voluntary guidelines identify risk areas and offer concrete suggestions to improve and enhance an organization's internal controls so that its billing practices and other business arrangements are in compliance with Medicare's rules and regulations.

As compliance programs have matured and new challenges have been identified, health care organization boards of directors have sought ways to help their organization's compliance program accomplish its objectives. Although health care organization directors may come from diverse backgrounds and business experiences, an individual director can make a valuable contribution toward the compliance objective by asking practical questions of management and contributing his/her experiences from other industries. While the opinion in *Caremark* established a Board's duty to oversee a compliance program, it did not enumerate a specific methodology for doing so. It is therefore important that directors participate in the development of this process. This educational resource is designed to assist health care organization directors in exercising that responsibility.

V. Suggested Questions for Directors

Periodic consideration of the following questions and commentary may be helpful to a health care organization's Board of Directors. The structural questions explore the Board's understanding of the scope of the organization's compliance program. The remaining questions, addressing operational issues, are directed to the operations of the compliance program and may facilitate the Board's understanding of the vitality of its compliance program.

STRUCTURAL QUESTIONS

1. **How is the compliance program structured and who are the key employees responsible for its implementation and operation? How is the Board structured to oversee compliance issues?**

The success of a compliance program relies upon assigning high-level personnel to oversee its implementation and operations. The Board may wish as well to establish a committee or other subset of the Board to monitor compliance program operations and regularly report to the Board.

2. **How does the organization's compliance reporting system work? How frequently does the Board receive reports about compliance issues?**

Although the frequency of reports on the status of the compliance program will depend on many circumstances, health care organization Boards should receive reports on a regular basis. Issues that are frequently addressed include (1) what the organization has done in the past with respect to the program and (2) what steps are planned for the future and why those steps are being taken.

3. **What are the goals of the organization's compliance program? What are the inherent limitations in the compliance program? How does the organization address these limitations?**

The adoption of a corporate compliance program by an organization creates standards and processes that it should be able to rely upon and against which it may be held accountable. A solid understanding of the rationale and objectives of the compliance program, as well as its goals and inherent limitations, is essential if the Board is to evaluate the reasonableness of its design and the effectiveness of its operation. If the Board has unrealistic expectations of its compliance program, it may place undue reliance

on its ability to detect vulnerabilities. Furthermore, compliance programs will not prevent all wrongful conduct and the Board should be satisfied that there are mechanisms to ensure timely reporting of suspected violations and to evaluate and implement remedial measures.

4. Does the compliance program address the significant risks of the organization? How were those risks determined and how are new compliance risks identified and incorporated into the program?

Health care organizations operate in a highly regulated industry and must address various standards, government program conditions of participation and reimbursement, and other standards applicable to corporate citizens irrespective of industry. A comprehensive ongoing process of compliance risk assessment is important to the Board's awareness of new challenges to the organization and its evaluation of management's priorities and program resource allocation.

5. What will be the level of resources necessary to implement the compliance program as envisioned by the Board? How has management determined the adequacy of the resources dedicated to implementing and sustaining the compliance program?

From the outset, it is important to have a realistic understanding of the resources necessary to implement and sustain the compliance program as adopted by the Board. The initial investment in establishing a compliance infrastructure and training the organization's employees can be significant. With the adoption of a compliance program, the organization is making a long term commitment of resources because effective compliance systems are not static programs but instead embrace continuous improvement. Quantifying the organization's investment in compliance efforts gives the Board the ability to consider the feasibility of implementation plans against compliance program goals. Such investment may include annual budgetary commitments as well as direct and indirect human resources dedicated to compliance. To help ensure that the organization is realizing a return on its compliance investment, the Board also should consider how management intends to measure the effectiveness of its compliance program. One measure of effectiveness may be the Board's heightened sensitivity to compliance risk areas.

OPERATIONAL QUESTIONS

The following questions are suggested to assist the Board in its periodic evaluation of the effectiveness of the organization's compliance program and the sufficiency of its reporting systems.

A. Code of Conduct

How has the Code of Conduct or its equivalent been incorporated into corporate policies across the organization? How do we know that the Code is understood and accepted across the organization? Has management taken affirmative steps to publicize the importance of the Code to all of its employees?

Regardless of its title, a Code of Conduct is fundamental to a successful compliance program because it articulates the organization's commitment to ethical behavior. The Code should function in the same way as a constitution, *i.e.*, as a document that details the fundamental principles, values, and framework for action within the organization. The Code of Conduct helps define the organization's culture; all relevant operating policies are derivative of its principles. As such, codes are of real benefit only if meaningfully communicated and accepted throughout the organization.

B. Policies and Procedures

Has the organization implemented policies and procedures that address compliance risk areas and established internal controls to counter those vulnerabilities?

If the Code of Conduct reflects the organization's ethical philosophy, then its policies and procedures represent the organization's response to the day-to-day risks that it confronts while operating in the current health care system. These policies and procedures help reduce the prospect of erroneous claims, as well as fraudulent activity by identifying and responding to risk areas. Because compliance risk areas evolve with the changing reimbursement rules and enforcement climate, the organization's policies and procedures also need periodic review and, where appropriate, revision.[4] Regular consultation with counsel, including reports to the Board, can assist the Board in its oversight responsibilities in this changing environment.

4 There are a variety of materials available to assist health care organizations in this regard. For example, both sponsoring organizations of this educational resource offer various materials and guidance, accessible through their web sites.

C. Compliance Infrastructure

1. Does the Compliance Officer have sufficient authority to implement the compliance program? Has management provided the Compliance Officer with the autonomy and sufficient resources necessary to perform assessments and respond appropriately to misconduct?

Designating and delegating appropriate authority to a compliance officer is essential to the success of the organization's compliance program. For example, the Compliance Officer must have the authority to review all documents and other information that are relevant to compliance activities. Boards should ensure that lines of reporting within management and to the Board, and from the Compliance Officer and consultants, are sufficient to ensure timely and candid reports for those responsible for the compliance program. In addition, the Compliance Officer must have sufficient personnel and financial resources to implement fully all aspects of the compliance program.

2. Have compliance-related responsibilities been assigned across the appropriate levels of the organization? Are employees held accountable for meeting these compliance-related objectives during performance reviews?

The successful implementation of a compliance program requires the distribution throughout the organization of compliance-related responsibilities. The Board should satisfy itself that management has developed a system that establishes accountability for proper implementation of the compliance program. The experience of many organizations is that program implementation lags where there is poor distribution of responsibility, authority and accountability beyond the Compliance Officer.

D. Measures to Prevent Violations

1. What is the scope of compliance-related education and training across the organization? Has the effectiveness of such training been assessed? What policies/measures have been developed to enforce training requirements and to provide remedial training as warranted?

A critical element of an effective compliance program is a system of effective organization-wide training on compliance standards and procedures. In addition, there should be specific training on identified risk areas, such as claims development and submission, and marketing practices. Because it can represent a significant commitment of resources, the Board should understand the scope and effectiveness of the educational program to assess the return on that investment.

2. How is the Board kept apprised of significant regulatory and industry developments affecting the organization's risk? How is the compliance program structured to address such risks?

The Board's oversight of its compliance program occurs in the context of significant regulatory and industry developments that impact the organization not only as a health care organization but more broadly as a corporate entity. Without such information, it cannot reasonably assess the steps being taken by management to mitigate such risks and reasonably rely on management's judgment.

3. How are "at risk" operations assessed from a compliance perspective? Is conformance with the organization's compliance program periodically evaluated? Does the organization periodically evaluate the effectiveness of the compliance program?

Compliance risk is further mitigated through internal review processes. Monitoring and auditing provide early identification of program or operational weaknesses and may substantially reduce exposure to government or whistleblower claims. Although many assessment techniques are available, one effective tool is the performance of regular, periodic compliance audits by internal or external auditors. In addition to evaluating the organization's conformance with reimbursement or other regulatory rules, or the legality of its business arrangements, an effective compliance program periodically reviews whether the compliance program's elements have been satisfied.

4. What processes are in place to ensure that appropriate remedial measures are taken in response to identified weaknesses?

Responding appropriately to deficiencies or suspected non-compliance is essential. Failure to comply with the organization's compliance program, or violation of applicable laws and other types of misconduct, can threaten the organization's status as a reliable and trustworthy provider of health care. Moreover, failure to respond to a known deficiency may be considered an aggravating circumstance in evaluating the organization's potential liability for the underlying problem.

E. Measures to Respond to Violations

1. What is the process by which the organization evaluates and responds to suspected compliance violations? How are reporting systems, such as the compliance hotline, monitored to verify appropriate resolution of reported matters?

Compliance issues may range from simple overpayments to be returned to the payor to possible criminal violations. The Board's duty of care requires that it explore whether procedures are in place to respond to credible allegations of misconduct and whether management promptly initiates corrective measures. Many organizations take disciplinary actions when a responsible employee's conduct violates the organization's Code of Conduct and policies. Disciplinary measures should be enforced consistently.

2. Does the organization have policies that address the appropriate protection of "whistleblowers" and those accused of misconduct?

For a compliance program to work, employees must be able to ask questions and report problems. In its fulfillment of its duty of care, the Board should determine that the organization has a process in place to encourage such constructive communication.

3. What is the process by which the organization evaluates and responds to suspected compliance violations? What policies address the protection of employees and the preservation of relevant documents and information?

Legal risk may exist based not only on the conduct under scrutiny, but also on the actions taken by the organization in response to the investigation. In addition to a potential obstruction of a government investigation, the organization may face charges by employees that it has unlawfully retaliated or otherwise violated employee rights. It is important, therefore, that organizations respond appropriately to a suspected compliance violation and, more critically, to a government investigation without damaging the corporation or the individuals involved. The Board should confirm that processes and policies for such responses have been developed in consultation with legal counsel and are well communicated and understood across the organization.

4. What guidelines have been established for reporting compliance violations to the Board?

As discussed, the Board should fully understand management's process for evaluating and responding to identified violations of the organization's policies, as well as applicable federal and state laws. In addition, the Board should receive sufficient information to evaluate the appropriateness of the organization's response.

5. What policies govern the reporting to government authorities of probable violations of law?

Different organizations will have various policies for investigating probable violations of law. Federal law encourages organizations to self-disclose wrongdoing to the federal government. Health care organizations and their counsel have taken varied approaches to making such disclosures. Boards may want to inquire as to whether the organization has developed a policy on when to consider such disclosures.

VI. Conclusion

The corporate director, whether voluntary or compensated, is a bedrock of the health care delivery system. The oversight activities provided by the director help form the corporate vision, and at the same time promote an environment of corporate responsibility that protects the mission of the corporation and the health care consumers it serves.

Even in this "corporate responsibility" environment, the health care corporate director who is mindful of his/her fundamental duties and obligations, and sensitive to the premises of corporate responsibility, should be confident in the knowledge that he/she can pursue governance service without needless concern about personal liability for breach of fiduciary duty and without creating an adversarial relationship with management.

The perspectives shared in this educational resource are intended to assist the health care director in performing the important and necessary service of oversight of the corporate compliance program. In so doing, it is hoped that fiduciary service will appear less daunting, and provide a greater opportunity to "make a difference" in the delivery of health care.

HIPAA Resources on the Web

Sarena Straus
www.mdx-med.com

Web Site	What It's About
www.hipaadvisory.com hippanews hippaalerts hippaadvisory hipaalive	Current HIPAA news along with alerts and a listserv with over 5000 members. Also has a glossary that identified HIPAA terminology. Has models, samples and templates. Joining the list also gives you access to other templates, PowerPoint presentations and sample forms.
http://www.cpr.net/hipaa/index.htm	Medical information portal that provides shortcuts to all of the HIPAA regulations.
http://corporate.findlaw.com	Under healthcare, enter your state and then search for HIPAA. Lists all HIPAA articles from findlaw.com.
Hipaablog.blogspot.com	BLOGS: personal web pages, formatted to resemble online journals. They can be excellent resources for current developments in the field. Here is a HIPAA Blog
www.cms.hhs.gov/hipaa/hipaa2/education/infoserie/	This site is full of HIPAA informational materials from HIPAA 101 to how to tell if you are a covered entity.
http://aspe.os.dhhs.gov/admnsimp/	Department of Health and Human Services.
Hipaa.org	Useful hyperlinks prepared by CMS in an easy to read format.
http://www.hipaa-dsmo.org/	Designated Standard Maintenance Organizations that maintain standards adopted by the Secretary.