

## My Brother's Keeper: The Rise of Independent Monitors



Geoffrey R. Kaiser, JD,  
Saul B Helman, MD, MBA

There has been a clear trend toward and increasing reliance upon the use of independent monitors in a range of circumstances by a wide array of agencies, both state and federal. From financial services to health care to the construction industry, monitors are appointed, typically though not always at the conclusion of a government investigation that has identified wrongdoing of some sort. The primary purpose: to scrutinize a company's compliance with laws and regulations, to assess a company's implementation of mandated remedial measures and to oversee a company's adherence to the terms and conditions of an agreement reached with the government to resolve existing or potential liability. They are known by a variety of names, depending on the particular case, and may be referred to as a Monitor, Examiner, Consultant, Compliance Officer or, in the health care context, an Independent Review Organization ("IRO") mandated by a Corporate Integrity Agreement ("CIA"). They are always independent third parties who are typically called upon to perform some type of policing function and to ensure maximum transparency by shining a bright light on the business operations of companies that have come under government scrutiny and, in some cases, have been charged with and even pleaded guilty to crimes. All forms of independent third party monitorships will be referred to as Monitors for purposes of this discussion.

The reason for the upward trend is in part due to the government's increased scrutiny of corporate America after Enron, a greater willingness on its part to hold corporations

accountable for the misdeeds of their employees, and more recently a shift in political landscape that favors more oversight. At the same time, the government's ability to appoint Monitors pursuant to agreements that provide for some type of pre-trial diversion without requiring a criminal prosecution gives the government much-needed flexibility to deal with corporate misconduct in a way that does not exact the ultimate penalty – a corporate guilty plea – which is frequently a death knell for a corporation that leads to the destruction of the business, the loss of thousands of jobs and, in some cases, even wider and more devastating economic and social consequences (the Arthur Andersen effect). The number of corporate monitorships authorized by the Department of Justice ("DOJ") since 1994, which has been pegged as the first year that DOJ appointed a corporate monitor, has steadily increased.<sup>1</sup> A similar trend can be seen in the health care industry. The number of corporate integrity agreements, certification of compliance agreements and settlement agreements with integrity provisions entered into by the Department of Health and Human Services ("HHS") has spiked upward in recent years. A total of 98 such agreements were entered into between 2000 and 2004, and almost four times that many – 377 – were entered into between 2005 and 2008. A great many of those agreements required a Monitor.<sup>2</sup>

The government's decision to appoint a Monitor is generally intended to reform past misconduct, ensure the probity of prospective corporate behavior and the integrity of the marketplace, and instill a culture

### Table of Contents

1	My Brother's Keeper: The Rise of Independent Monitors
5	Export Controls and Life Sciences Companies
8	Current Pedigree Requirements and the Potential Future of e-Pedigree
11	The Board of Directors Role in Overseeing Compliance Program Effectiveness

<sup>1</sup> Corporate Counsel Magazine, "Someone to Watch Over Me" (October 2007).

<sup>2</sup> U.S. Department of Health and Human Services, Office of Inspector General, Corporate Integrity Agreements Document List.

of compliance and good corporate citizenship in organizations that have, in one way or another, fallen short of statutory requirements, regulatory requirements, industry guidance, and/or the government's expectations. The basis for the Monitor's authority is often, though not invariably, a deferred prosecution agreement ("DPA"), a non-prosecution agreement ("NPA"), or a CIA.

Sometimes, two Monitors can be appointed, one under authority of one agreement and one under authority of the other, which has been a relatively rare occurrence. Dual appointments were made, however, when the United States Attorney's Office for the District of New Jersey resolved the criminal investigations of several medical device companies who allegedly violated the anti-kickback statute through their financial arrangements with surgeons using their products. There, each company was required to execute both a DPA requiring a monitor and a CIA requiring an IRO. In some cases, a Monitor will be appointed pursuant to a Consent Decree entered by a court, or appointed by a government agency to oversee a major public works project to ensure that the project is performed to specifications and is not impacted by fraud or other corrupt influence.

The scope of the Monitor's authority may be sweeping, or may be more circumscribed, depending on the agency involved and the terms of the particular authorizing document at issue. The costs of the Monitor – which can be enormous – are ordinarily, though not always, borne by the entity that is subject to the monitorship. Who actually selects the Monitor varies widely. In some cases, the Monitor is selected by a government agency with little or no input from the company to be monitored, while in other cases the company makes the selection subject to government approval. In still other cases, a hybrid selection process is used, with the government screening candidates for consideration by the company, and the company weighing in with its own preferences and, in some cases, even wielding a veto over a candidate that the company views as unacceptable. The duration of a monitorship also can vary greatly, depending on the circumstances that led to

the Monitor's appointment. The Monitor's term may be as short as a year or may endure for a number of years. A prosecution agreement may provide for the possible extension of a monitorship if circumstances warrant or, conversely, may authorize early termination of a monitorship if the objectives of the monitorship have been satisfied and there is no longer a need for a Monitor. Monitors are required to make periodic reports to the government, and often to the monitored entity as well. In some cases, the Monitor may also report to third-party regulators.

In the case of Monitors appointed in criminal cases, in March 2008, the DOJ promulgated guidance for Each United States Attorney's Office around the country concerning the selection and use of Monitors that are mandated by DPAs and NPAs reached with corporations. The guidance sets forth a series of principles that are intended to guide prosecutors in the areas of Monitor selection, scope of Monitor responsibilities, and monitorship duration. In the area of selection, the guidance requires that Monitors be selected on merit, and that actual and potential conflicts of interest be avoided. The guidance urges the government and the corporation to consult on the role of the Monitor and the skills and expertise he or she should possess. The guidance also suggests, where practical, that a Monitor should be selected from a pool of at least three qualified candidates. Each United States Attorney's Office around the country is required to create a standing or ad hoc committee of prosecutors to consider the selection or veto of all Monitor candidates, and that committee must include the Office Ethics Advisor, the Chief of the Criminal Division, and at least one other prosecutor. However, it should be stressed that while these guidelines establish factors that must be considered by prosecutors in the selection process, the guidance pointedly does not mandate a uniform method of choosing Monitors, nor is there a standardized system for advertising monitorship opportunities. This fact has generated criticism as well as the perception among many that monitors are members of an exclusive 'club' and that monitorships are handed out as favors to a privileged few who are well-

connected enough to be accepted into the 'club' as members.

The guidance, issued as memorandum, titled, "Selection and Use of Monitors in Deferred Prosecution Agreements and Non-Prosecution Agreements with Corporations," included guidelines to prosecutors to evaluate the use of Monitors in the context of the potential benefit to the corporation and public, and the potential cost to the corporation and related impact to the business. Principles related to engagement of Monitors in these situations reflect the reaction by companies to historical appointments and public concerns include:

1. Identification and agreement between the government and company on the qualifications/requirements prior to appointment, i.e., a needs based appointment;
2. Independence of the Monitor relative to the company and/or government;
3. Monitor focus on the terms/requirements/scope of the agreement;
4. Actions of Monitor directed to preventing misconduct that led to the agreement;
5. Periodic written reports provided to the government by the Monitor;
6. Any company actions that lead to a lack of adherence to Monitor recommendations or requirements must be reported to the government;
7. Monitor has the right to report other misconduct;
8. Duration of the agreement should be determined by the time required for the company to implement and adhere to the agreement;
9. Duration of agreement subject to changes in circumstance. Within four days of the guidance being issued, a Congressional Hearing was held that focused on "Deferred Prosecution: Should Corporate Settlement Agreements Be Without Guidelines?" and while acknowledging the recent issuance of the guidance described above, issues were discussed including:
  - a. Appointment of Monitors without any

public notice, bidding, or assessment of qualifications required;

- b. Potentially significant cost burden to company, with no cost guideline in place;
- c. No laws or guidance govern the role of Monitors; and
- d. Monitors could act as prosecutor, judge and jury.

When performed correctly, a monitorship can be a tremendous benefit to the monitored entity, to the government, and to the general public. Past misdeeds can be remedied, trust and integrity can be restored, and remedial measures can be implemented to instill a culture of compliance and prevent future misconduct. Companies previously laboring under a cloud of criticism, and suffering from eroding stock prices and declining employee morale, can see their reputations restored and their market share return. Of course, the appointment of a monitor is not a panacea, and monitor oversight is not a guarantee that past misconduct will be reformed. Nor does the appointment of a monitor invariably result only in benefits. After all, requiring a company to accept a monitor, while unquestionably justified and even necessary in many instances, is a significant intrusion into that company's business. If care is not taken in defining a monitor's scope of responsibility and authority, the very act of performing the monitorship can unduly interfere with business operations and cause more harm than good.

Implementation of a settlement agreement and the incorporation of a monitorship can be a significant burden to the business operation, especially in cases where a compliance program has not necessarily been integral to the company up to that point. A company might find itself in a situation where there are new barriers to decision making, a lack of insight into business operations and related cycles, rulings or requirements that are at odds with business practice, and an increasing cost center that does not appear to add value to the business. These situations frustrate leadership and can lead to a lack of executive support for developing compliance organizations,

which can inhibit effective implementation of an agreement's compliance-related requirements and defeat the purpose underlying the appointment of a monitor.

The agreements containing monitorship provisions have been increasing in complexity and sophistication, with recent examples in health care that have required Board-level certifications, executive-level certifications, and more detailed requirements in reporting. The role of Monitors also appears to have broadened, with some Monitors actively involved in the day-to-day operations, and on-site and in-field monitoring. Failure of an organization to embrace a settlement agreement and actively learn from the Monitor diminishes the real value these agreements and Monitors can and should provide. The agreement can be viewed as a roadmap to a comprehensive and sustainable compliance program and, if implemented faithfully, is potentially an insurance policy for any future investigation. Agreements might have an element of 'cut-and-paste' from agreements of other companies, and there are usually a few areas open to interpretation; however, attempts to renegotiate or swing interpretation in favor of the company can sometimes impede progress and alter perception adversely. Assuming executive leadership support is secured, the priorities of the Chief Compliance Officers are to:

- » appoint/recruit a project manager as soon as (or in anticipation of) a settlement agreement being signed
- » coordinate with Human Resources for reassignment or recruitment of compliance talent
- » coordinate with Legal to determine need for 'privilege'
- » coordinate with Information Technology for prioritized support as needed
- » identify external consultants for advisory and implementation support as needed, bringing an outside and current perspective
- » drive a culture of compliance
- » hold people accountable
- » prevent, detect, correct non-compliance

Despite potential areas of conflict and concern related to Monitors, the experience to date reflects an overall benefit of monitorships, providing and reinforcing compliance program commitment, transparency, and sustainability, and if leveraged well, the Company can derive significant insight, implementation resources and rapid shift to a culture of compliance. The Monitor can be a tremendous resource to provide industry compliance awareness and current trends, help define expectations and support clarification of areas of ambiguity in the agreement, identify areas of risk and related prioritization, and reinforce the need for executive leadership support.

# Export Controls and Life Sciences Companies



**Urszula Zapolska, Associate Director**

**Denise Walker, Associate Director**

## Background and Introduction

The U.S. government maintains export controls on certain chemicals, equipment, materials, software, technology, and manufacturing plants. Similarly, export of certain microorganisms, toxins, biological equipment, and related technology is controlled by the government. These controls are in place to further U.S. foreign policy interests in opposing the proliferation and use of biological and chemical weapons. Other countries, including those in the European Union, have similar controls in place. U.S.-based life sciences companies, particularly those involved in exporting or re-exporting medical devices; some laboratory, medical, or manufacturing equipment; or chemicals, toxins, pathogens, and biologics need to be concerned with export controls and activities of the Bureau of Industry and Security (“BIS”). A BIS-issued license may be required for these companies’ exports depending on the items being exported, their destination, and use.

BIS is one of the primary agencies controlling the U.S. exporting and re-exporting activities by implementing and enforcing the Export Administration Regulations (“EAR”). BIS regulates “dual-use” items, which are items with both commercial and military or proliferation applications; and whenever required, issues appropriate licenses. Dual-use items may include commercial items without an obvious military use in a form of commodities, technology, and software including some of the products manufactured by life sciences companies.

Specifically, the BIS-issued licenses are required to export anywhere in the world certain toxins, pathogens, genetically modified microorganisms, and the technology for their production and/or disposal. Additionally, BIS requires a license for the export to specified countries commercial equipment and materials that can be used to produce biological agents and related production technology. The Commerce Control List (“CCL”) prepared by BIS lists 12 entries that

are subject to biological controls.

BIS issues licenses for export of certain chemicals, which can be used in the production of toxic chemical warfare agents; as well as relevant process control software; technology for the use, production, and/or disposal of such items; and the facilities designed to produce them. License is also required for export of certain chemical manufacturing facilities and equipment, toxic gas monitoring systems, and detectors that can be used in the production of chemical warfare agents, and the technology for the use of such items. In all, CCL has 14 entries that are subject to chemical controls.

In Fiscal Year 2007, the most recent year for reported data, BIS processed 19,512 export license applications involving trade worth approximately \$52.6 billion. About 7% of all applications were for the export or re-export of biological agents and equipment. The value of these exports exceeded \$65 million. At the same time, 13% of all license applications were for the export or re-export of chemical precursors and equipment. The value of these exports exceeded \$809 million.

BIS is not the only agency that regulates exports. In fact, BIS often cooperates with other agencies including the Federal Bureau of Investigation, the Department of State (which has the authority over defense articles and services), the Department of Treasury Office of Foreign Assets Control, U.S. Customs, and the Food and Drug Administration (with authority over export of unapproved medical devices). BIS is considered an active agency. In 2007, BIS investigations resulted in the criminal conviction of 16 individuals and businesses for export and anti-boycott violations, with penalties totaling more than \$25.3 million in criminal fines, over \$1.4 million in forfeitures, and 324 months of imprisonment. Furthermore, during the same time, BIS completed 75 administrative cases against individuals and businesses and issued over \$6 million in administrative penalties.

- » On December 31, 2008, the Commerce Department's Bureau of Industry and Security (BIS) announced that Buehler Ltd, a manufacturer of scientific equipment and supplies from Lake Bluff, Illinois, has agreed to pay a \$200,000 civil penalty to settle allegations that it made 81 unlicensed exports of a lubricant containing Triethanolamine (TEA) in violation of the Export Administration Regulations. Unlicensed export of this same substance was the cause of an \$115,000 civil penalty assessed against another Illinois manufacturing company in October 2008.<sup>3</sup>
- » In the December 2008 press release, BIS Under Secretary of Commerce stressed, "Targeted and effective controls on materials that could be used in biological and chemical weapons are critical to preserving U.S. national security. [...] Companies should be mindful of the chemical make-up of their exports."<sup>3</sup>
- » In July 2008, Select Engineering, Inc. was fined for selling and transporting medical electrode sensor elements and stainless steel snap connectors from U.S. to Iran.<sup>3</sup>
- » In August 2005, Maine Biological Labs was sentenced to a criminal fine of \$500,000 and five years of probation for illegal exports of virus toxins to Syria.<sup>3</sup>
- » In March 2008, MTS Systems Corporation was fined \$400,000 and placed on probation for two years for omitting the nuclear end-use for the seismic testing equipment in its submission for license application to BIS.<sup>3</sup>
- » In 2002, Sigma-Aldrich Corporation and two of its subsidiaries paid a \$1.7 million fine to settle charges involving illegal exports of biological toxins. The Commerce Department had instituted administrative enforcement actions against the Sigma-Aldrich companies alleging that a company they had acquired in 1997 had made unauthorized exports of controlled biological toxins to Europe and Asia on numerous occasions prior to the

acquisition and had continued the unlicensed exports for more than a year after the acquisition.<sup>3</sup>

BIS has also made clear that businesses can be held liable for any violation of the EAR committed by companies they acquire. Accordingly, businesses are advised to perform due diligence in scrutinizing the export control practices of companies they plan to acquire. This review should include company's export history and compliance practices and procedures including product classifications, technology exchanges, export licenses, end use and end users, and the status of foreign employees with access to restricted technologies.

#### **What does this mean to the industry?**

The responsibility for export compliance always rests with the exporter. Knowing whether your company's exports are subject to export controls is critical in avoiding fines, administrative sanctions including loss of export privileges, and criminal charges.

#### **What is considered an export?**

Any item sent from the U.S. to a foreign destination is an export, regardless of the method used for transfer, and includes both shipments of products as well as internet downloads. An item is considered an export even if it is sent outside the U.S. temporarily, as a gift, or to a wholly-owned U.S. subsidiary in another country. Even a foreign-origin item which has been transmitted or trans-shipped through the U.S. or being returned from the U.S. to its foreign country of origin is considered an export.

BIS also recognizes so-called "deemed exports," which is an exportation of technological knowledge by releasing technology or source code that has both military and civilian use (even if the dual use is not obvious) to a foreign national in the U.S. Deemed exports have particular relevance to companies in the biotechnology, pharmaceutical, and medical device industries, as they outsource research and development activities to foreign-based companies and hire non-US citizens for this type of activities.

<sup>3</sup> Source: [www.bis.doc.gov/news](http://www.bis.doc.gov/news).

### **How to determine when a BIS license is needed?**

When considering whether a company's exports require BIS-issued license, the following questions need to be answered:

1. *What* is exported?

- » Determine whether exports have dual-use applications and, as such, are subject to BIS administration.
- » Assess whether an export license is needed by determining a product's *Export Control Classification Number ("ECCN")* and cross-referencing the ECCN against the *Commerce Control List (CCL)*. The ECCN is an alphanumeric code, e.g., 3A001, which describes a particular item or type of item and indicates the controls placed on that item and applicable license exceptions. The appropriate ECCN must be listed on export documentation. ECCNs are periodically revised, and items are added or taken from the CCL.
- » Evaluate if items fall under the BIS jurisdiction but are not listed on the CCL, designated as EAR99, which typically are low-technology consumer goods that most often do not require a license for export. However, if these items are exported to an embargoed country, to an end-user of concern, or in support of a prohibited end-use, a license may still be required.

2. *Where* are the items going?

- » Consider if an item is to be sent to one of the embargoed countries and countries designated as supporting terrorist activities (Cuba, Iran, North Korea, Sudan, and Syria). Virtually all exports to these countries require licenses. For other countries, restrictions for export vary. Moreover, some products have worldwide restrictions.

- » Determine whether license is needed based on the "reasons for control" of the item and the country of ultimate destination for items with ECCN other than EAR99. To do this, compare the ECCN with the Commerce Country Chart. If there is an "X" in the box based on the reason(s) for control of your item and the country of destination, a license is required (unless a license exception is available).

3. *Who* will receive these items?

- » Review whether or not the item is to be shipped to certain individuals and organizations prohibited from receiving U.S. exports.
- » Review whether or not the recipient may receive goods if a license is obtained. The company intending to export an item must ensure that no proscribed individuals will be involved with the transactions.

4. *How* are the items used? What is the end-use for the items exported?

- » Determine if the end-use, particularly any uses related to proliferation activities, including chemical and biological, is prohibited or requires a license.
- » Refer to Part 744 of the EAR, which provides more information on the specific regulations related to end-user and end-use controls.

Applications for BIS-issued licenses can be done online or through U.S. mail. Detailed information related to the process of obtaining licenses, as well as links to EAR, CCL, and additional guidance are provided on the BIS website at [www.bis.doc.gov](http://www.bis.doc.gov).

# Current Pedigree Requirements and the Potential Future of e-Pedigree



**Carol Landsman, Director**

**Gregory V. Page, PhD, Managing Director**

The ability to demonstrate quality manufacturing, safe distribution and effective recall of pharmaceutical products is of growing concern throughout the world and a business imperative for any pharmaceutical manufacturer. High profile incidents in the industry, well touted in the media, illuminate the hazards of compromised product integrity: a highly anticipated new drug causes life-threatening side effects during first-in-human clinical trials; two large pharmacy chains are found guilty of selling expired products; an important intravenous solution is contaminated due to a supplier issue; a major lifestyle drug faces counterfeiters in the market. The results can be devastating to product, patient and pharmaceutical manufacturer. It is not only critical for a pharmaceutical manufacturer to be able to secure their drug supply chain against counterfeit, diverted, subpotent, substandard, adulterated, misbranded or expired drugs, but also definitively demonstrate compliance and competence with applicable state, federal and international rules, laws and regulations to a outside authority. The pedigree requirements and processes are one such set of regulations that pharmaceutical manufacturers must have to assure definitive and demonstrable systems and processes in the event of a product recall or otherwise market place removal.

In the United States, most individual state requirements related to drug distribution safety require the creation of a drug pedigree. A drug pedigree is a certified record that documents the distribution of a prescription pharmaceutical. It answers questions related to the chain of custody of the prescription drug including, what, where, when and why. It usually begins by recording the sale of a prescription pharmaceutical by a manufacturer, includes all additional acquisitions and sales by wholesalers

and repackagers, and includes final sale to a pharmacy or other entity administering or dispensing the drug.

A drug pedigree works by providing transparency and accountability for all persons who handle the prescription drug; however, issuing a drug pedigree alone without “secure pedigree transactions,” does not necessarily result in a more secure pharmaceutical supply network. The drug pedigree laws usually specify what information, both static and dynamic, is required to appear on the pedigree itself. In addition, the laws require a certain degree of assurance that the pedigree is securely updated and sent between trading partners in a secure manner. They also require that recipients of the product authenticate it to the drug pedigree.

One way to increase the “security” of the pedigree is to generate and track the pedigree information electronically. California has been proposing stringent requirements for electronic drug pedigree, including three unique requirements that directly affect pharmaceutical and biologics manufacturers: (1) the manufacturer must initiate the pedigree, (2) the drug pedigree must be maintained in an electronic interoperable system, and (3) the product must be identified with a unique serial number.<sup>4</sup> Although implementation of these requirements continues to be postponed (it is now targeted for January 1, 2011), it is clear that some form of electronic pedigree will become a requirement for drug manufacturers at some future date.

The benefits of electronic pedigree are significant and important, in both a business and compliance framework. First, an electronic pedigree is much harder to falsify than a paper-based pedigree given the secure nature of electronic systems. Second,

<sup>4</sup> California Board of Pharmacy e-Pedigree Requirements, (March 2008).

the certification requirements as part of the electronic pedigree receipt process should result in heightened control and oversight by the recipient. Third, electronic pedigree provides for an easily retrievable audit trail in the event such action is necessary. Fourth, electronic pedigree in itself requires an element of sophistication, and as such, is a barrier to potential counterfeiters who tend to be opportunistic. Finally, electronic pedigree can be implemented with just lot-level tracing as an interim step while item-level serialization is being planned.

The new global economy has contributed to a rise in counterfeit drugs. More than 10% of global pharmaceutical commerce is counterfeit with sales of fake drugs passing \$40 Billion last year.<sup>5</sup> Without adequate safeguards, the Food and Drug Administration (“FDA”) has estimated that sales from counterfeit drugs will reach \$75 Billion by 2010 with 10-30% most likely counterfeits from developing countries with weak regulatory systems. The primary channels for counterfeit drugs since 2002 and the weakest links in the supply chain have been via unregulated, illegal Internet-based entities, gray market diversion, re-importing and packaging activities. In fact, one of the most widely publicized cases of counterfeit prescription drugs happened in 2003 when the FDA issued a recall of three lots of Lipitor which had been repackaged by a secondary wholesaler. In 2003, three counterfeit lots of the anemia drug Procrit were discovered in the United States prompting another FDA recall. In 2005, another warning was issued regarding counterfeit lots of Lipitor, Viagra and Evista. Since 2005, many United States pharmaceutical manufacturers have instituted track and trace practices across their entire supply chain thereby reducing the amount of major recalls and incidents of counterfeit prescription drugs in the national pharmaceutical distribution system, thereby validating the effectiveness of self-regulation through pedigree.

In June, 2008, the brand protection firm MarkMonitor released its latest “brandjacking index” where they found that more than 20,000 websites are abusing drug trademarks. Many consumers unknowingly ex-

pose themselves to counterfeit prescription drugs through the use of unregulated, illegal, Internet-based entities. In May of 2007, the FDA published a warning naming 24 websites possibly involved in distributing counterfeit Xenical, Tamiflu and Cialis.

Regulatory agencies throughout the world have been attempting to address the issue of protection of the integrity of pharmaceutical products and their supply chains for over 20 years with limited success due to limitations in technology and industry pressures, as well as inconsistencies between international, federal, and state legislation;

- » In 1987 Congress passed the FDA Prescription Drug Marketing Act (“PDMA”) requiring drug distributors to document via a pedigree (paper or electronic) the chain of custody as drug products move through their distribution systems; the regulation advocates but does not require the use of Radio Frequency Identifications (“RFID”); the FDA decided to stay these requirements until more modern methodologies became available.
- » As a result of the ineffectiveness of PDMA, several states including Florida and California have since enacted their own laws for drug pedigrees; California is the only state requiring electronic pedigrees across manufacturers distributors and retailers, but the industry has lobbied to extend the California compliance date from 2009-2011 due to their inability to implement an electronic system by that date.
- » In September, 2007 the Food and Drug Administration Amendments Act (“FDAAA”) was signed into law requiring the Secretary of the Department of Health and Human Services (“HHS”) to develop standards and validate technologies for the purpose of securing the drug supply chain; standards developed under this ruling shall address promising technologies.
- » In April, 2008, the House of Representatives introduced the Safeguarding Pharmaceuticals Act of

<sup>5</sup> FDA Anti-Counterfeiting Report (2006).

2008 (“HR5839”) to bolster the safety and security of the pharmaceutical supply chain which requires the FDA to generate a unified pedigree standard that companies would then need to use to track and trace pharmaceuticals as they traverse the supply chain.

- » FDA is now the only national regulatory and enforcement authority looking closely at an e-pedigree requirement and the FDA has the opportunity to set a nationwide standard for an e-pedigree system as well as which technology should be used and what policies should be in place for enforcement; however the appropriate technology has not been developed as yet so the FDA continues to extend the standards’ deadline.
- » In Europe there is also a concern regarding supply chain integrity emphasizing improvements at the point of drug dispensing. Many countries including Italy, Belgium, Portugal, Spain, the Netherlands and France have requirements related to drug pedigree, limiting the ability to enact a common and effective solution across Europe. Recently the European Federation of Pharmaceutical Industries and Associations (“EFPIA”) endorsed the use of 2D Data Matrix Bar Code as the common data carrier across Europe.

Although specific aspects of the regulations are in flux, current interpretations of the 1987 PDMA and 2007 FDAAA acts, as well as the actual market place experiences of past events, clearly set expectations by state and federal government and the public that pharmaceutical manufacturers and distributors must be able to ensure the safety and security of their supply chain from raw material procurement to finished goods distribution.

The ability of pharmaceutical company management to be able to track and trace all of its products at any point in the supply chain is now a basic requirement. When the e-pedigree regulations are enacted at the state and/or federal level, those companies with validated, operationally sound, auditable pedigree programs will be able to develop appropriate, cost-effective solutions within the regulatory framework and defined timelines. In fact, the lack of an appropriate pedigree framework is a common pitfall for many companies and usually comes to light only during the worst times such as product-related adverse events or product recall actions.

# The Board of Directors Role in Overseeing Compliance Program Effectiveness



David M. Yarin, Director

## Introduction

Recent corporate integrity agreements (“CIAs”) from the Office of Inspector General (“OIG”) including Tenet Healthcare Corporation (November 2006), Cephalon, Bayer and Eli Lilly have required Boards of Directors to be responsible and accountable for the effectiveness of their organizations’ compliance programs. Specifically, the CIAs have required Boards (or their compliance subcommittees) to adopt a resolution certifying to the effectiveness of their organizations’ compliance program, including the performance of a compliance program effectiveness review. Tenet’s CIA included the requirement for the Board’s compliance subcommittee to retain an independent compliance advisor, while Bayer’s CIA requires the organization to implement a compliance expert panel. Eli Lilly’s recent CIA requires, among other things, that the committee of the Board of Directors annually reviews the company’s compliance program and certify to its effectiveness, and that certain managers annually certify that their departments or functional areas are compliant. “OIG’s Corporate Integrity Agreement will increase the transparency of Eli Lilly’s interactions with physicians and strengthen Eli Lilly’s accountability for its compliance with the law,” said Department of Health and Human Services Inspector General Daniel R. Levinson. In light of these regulatory developments, this article discusses:

- » What constitutes an effective compliance program?

- » How should a compliance program effectiveness review be performed?
- » Which practical activities should be considered for meeting a Board’s fiduciary responsibility regarding oversight of compliance program effectiveness?

For this article, the term “Board” may refer to the Board of Directors or a subcommittee of the Board that focuses on compliance matters.

## Effective Compliance Programs

Recent CIAs have made organizations’ Board of Directors specifically responsible for the oversight of compliance program effectiveness. By requiring the adoption of a resolution certifying to compliance program effectiveness, the OIG is essentially ensuring that Boards (typically through a subcommittee that focuses on compliance) have the ultimate responsibility for their organizations maintenance of an effective compliance program. Prior to these CIAs, the OIG offered recommendations for Board oversight in this area through compliance program guidance and publications (e.g., the OIG/American Health Lawyers Association or “AHLA” paper entitled, “Corporate Responsibility and Corporate Compliance: A Resource for Health Care Boards of Directors”). But with these CIAs turning prior recommendations into requirements, greater focus has been placed on the Board’s oversight of an organization’s compliance program. The table below summarizes relevant CIA requirements:

ORGANIZATION	CIA DATE	INDEPENDENT COMPLIANCE ADVISOR OR COMPLIANCE EXPERT PANEL	QUARTERLY COMPLIANCE PROGRAM REVIEW	ANNUAL COMPLIANCE PROGRAM EFFECTIVENESS REVIEW	COMPLIANCE PROGRAM EFFECTIVENESS RESOLUTION
Tenet Cephalon	September 2006	X		X	X
Bayer	November 2008	X		X	X
Eli Lilly	January 2009		X	X	X

However, beyond the requirement to certify compliance program effectiveness, the key for the Board is to review information that supports the determination that a compliance program is effective. The OIG’s guidance and publications mentioned previously provide the outline for making this determination. Determining compliance program effectiveness begins by looking at each of the OIG’s seven (7) elements areas (as described in the OIG’s Compliance

Program Guidance) and reviewing related information for each element. The OIG has provided questions to consider when evaluating compliance program effectiveness in supplemental guidance and in a joint publication with the AHLA. While the following table is not meant to be all-inclusive in determining compliance program effectiveness, it highlights each of the seven (7) element areas and considerations in the OIG guidance and joint AHLA publication:

COMPLIANCE PROGRAM ELEMENT	DESCRIPTION	CONSIDERATIONS FOR DETERMINING EFFECTIVENESS
High-level Oversight	Reporting structure for Chief Compliance Officer; Board-level and management compliance committees	<ul style="list-style-type: none"> <li>» Does the compliance officer have direct access to the governing body, the president or CEO, all senior management, and legal counsel?</li> <li>» Does the compliance officer make regular reports to the board of directors and other management concerning different aspects of the organization’s compliance program?</li> </ul>
Written Standards/Policies and Procedures	Code of Conduct; compliance-related policies (e.g. non-retaliation, investigating compliance issues)	<ul style="list-style-type: none"> <li>» Have the standards of conduct been distributed to all directors, officers, managers, employees, contractors, and vendors?</li> <li>» Has the organization developed a risk assessment tool, which is re-evaluated on a regular basis, to assess and identify weaknesses and risks in operations?</li> </ul>
Training and Education	Examples include training for industry and identified risk areas	<ul style="list-style-type: none"> <li>» Has the organization evaluated the appropriateness of its training format by reviewing the length of the training sessions; whether training is delivered via live instructors or via computer-based training programs; the frequency of training sessions; and the need for general and specific training sessions?</li> </ul>
Auditing and Monitoring	Auditing – testing performed by a party independent of the function being tested; Monitoring – testing/ data review which can be performed by the department – results reported to Compliance and/or Audit Departments	<ul style="list-style-type: none"> <li>» Is the audit plan re-evaluated annually, and does it address the proper areas of concern, considering, for example, findings from previous years’ audits, risk areas identified as part of the annual risk assessment, and high risk areas?</li> </ul>
Open Lines of Communication	Anonymous channels to report compliance-related issues, questions or concerns	<ul style="list-style-type: none"> <li>» Has the organization established a well-publicized, anonymous hotline or other similar mechanism so that employees, contractors, and other individuals can report potential compliance issues?</li> <li>» Are the results of internal investigations shared with the governing body and relevant departments on a regular basis?</li> </ul>
Responding to Detected Deficiencies	Explicit procedures to investigate and report (if necessary) compliance-related matters	<ul style="list-style-type: none"> <li>» Has the organization created a response team, consisting of representatives from the compliance, audit, and any other relevant functional areas, which may be able to evaluate any detected deficiencies quickly?</li> </ul>
Enforcement of Standards	Non-hiring or retention of individuals or third-parties who have been excluded from participating in Federal Healthcare Programs; disciplinary action (up to and including termination, if necessary) for compliance-related violations	<ul style="list-style-type: none"> <li>» Are employees, contractors and vendors checked routinely (e.g., at least annually) against government sanctions lists, including the OIG’s List of Excluded Individuals/Entities (LEIE) and the General Services Administration’s Excluded Parties Listing System?</li> <li>» Are disciplinary standards established which describe disciplinary action (up to and including termination) for compliance-related violations?</li> </ul>

The key is not merely answering “yes” to the above questions, but to perform a comprehensive review that

1. builds the basis, support and documentation for the “yes” answer,
2. builds the data to demonstrate that activities are meeting defined or acceptable targets, and
3. “makes the case” for determining that a compliance program is effective.

In addition to performing a compliance program review, the Board should receive regular updates from the Chief Compliance Officer (“CCO”) as to compliance program activities and metrics in each of the seven (7) element areas, along with updates as to

ongoing compliance matters such as significant investigations. Although the following table is not meant to be all-inclusive, suggested information/data that the CCO should provide to the Board includes but is not limited to:

SEVEN ELEMENT AREA	DATA PROVIDED BY THE CCO	FREQUENCY
High-level Oversight	» Proposed changes to Board Compliance Committee charter	» Every two (2) years or as needed » Annually; or upon change in personnel or as needed » Annual
Written Standards	» Proposed revisions to Code of Conduct » Proposed new compliance policies; summary of changes to existing compliance policies » Proposed changes to policies which would alter compliance information provided to the Board » Explicit policies regarding types of and when, how, and by whom compliance matters will be reported to the Board	» Every two (2) years or as needed » Ongoing » Ongoing; as needed » As needed
Training and Education	» Data to support tracking of compliance training completion and attendance » Summary of training content and delivery methods » Board training on industry risks and enforcement activities	» Ongoing; as needed » Ongoing; as needed » As needed; annually at a minimum
Auditing and Monitoring	» Annual compliance audit work plan incl. risk assessment results and OIG work plan review » Compliance audit results incl. management corrective action when applicable	» Annually » Ongoing
Open Lines of Communication	» Number of hotline calls, number of open and closed investigations, significant reports received (e.g. involving senior management), report trends (e.g. by report category)	» Ongoing
Responding to Detected Deficiencies	» Updates as to key investigations or significant compliance matters identified	» Ongoing
Enforcement of Standards	» Summary of ongoing exclusion check results » Summary of disciplinary actions taken for compliance-related violations	» Ongoing

Much of the above information can be provided in a “dashboard” format that provides for consistent and succinct reporting.

## Performing a Compliance Program Effectiveness Review

In making a determination as to whether a compliance program is operating effectively, a Board should request the performance of a comprehensive review of program activities, which includes reviewing the program updates and information provided by the CCO. The review should be performed by persons independent of the compliance program, so as to provide the Board with an objective analysis. The review should include but not be limited to the following:

- » Understanding of how the compliance program operates and key activities in

each of the seven (7) element areas and key risk areas

- » Testing of key compliance program activities (e.g., investigation of hotline reports)
- » Comparison of information obtained and testing results to a compliance program effectiveness framework (e.g., OIG Compliance Program Guidance)
- » Management corrective actions planned or implemented to deficiencies and improvement opportunities identified
- » Conclusion as to overall compliance program effectiveness

Compliance program activities can be tested in various ways. The table below, while not all-inclusive, provides examples of suggested testing steps and information/data to focus on in each of the seven (7) element areas:

ELEMENT	TESTING STEP	FOCUS
High-level Oversight	» Review of CCO Job Description	» Reports to CEO and dotted-line to Board (not General Counsel or CFO) » Authority to investigate and retain counsel
Written Standards	» Code of Conduct review	» Includes non-retaliation policy » Covers risk areas relevant to organization » Easy to read
Auditing and Monitoring	» Review of past year's compliance audits	» Audits clearly define and identify testing error rates » Includes management corrective actions where applicable
Training and Education	» Employee survey	» Questions to confirm retention of training content
Open Lines of Communication	» Independent review of sample of hotline call investigations and documentation	» Confirm timeliness and thoroughness of compliance report investigation and supporting documentation
Responding to Detected Deficiencies	» Confirm if re-payment, reporting (e.g. reportable event if under a CIA) and other corrective action steps were met	» Confirm if appropriate mitigation steps were taken (include with above compliance report review)
Enforcement of Standards	» Select sample of new hires and existing personnel to confirm exclusion check performance and appropriate follow-up (if a match was identified)	» Existence of documentation to support performance of exclusion check and appropriate follow-up steps, if necessary.

## Fiduciary Responsibility of the Board

While the *Caremark* decision and OIG Guidance/Publications have helped to clarify the Board's role in compliance program oversight, there are practical considerations that management should follow in making the Board's oversight effective. 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."<sup>5</sup>

Considerations for Board oversight include:

- » Compliance program reports to the Board should be timely and in a consistent, succinct format
- » Compliance reporting to the Board should focus on management's analysis of the data and information available, and include corrective actions for deficiencies identified. The Board should not be left to make the analysis on their own from only raw data or information (i.e., management should tell the Board "the story").
- » Keep it simple. Directors/Board-level committee members typically have

numerous topics to cover in a limited period of time, with compliance being only one topic. Bar charts and graphs are wonderful presentation tools, but should be provided only if the takeaway from the data is clearly presented both verbally and/or on any presentation or handout materials.

- » Explicit policies/procedures should define what types and how, when and by whom certain matters are reported to the Board. For example, compliance reports that involve senior management, whether substantiated or unsubstantiated, should be communicated properly and promptly to the Board (or Board Chair). Compliance reporting should be handled responsibly so that unsubstantiated reports are initially communicated as allegations only, with an investigation and updates to the Board to follow.
- » Boards should receive updates and education on industry risk areas, enforcement priorities and activities.
- » Whether subject to a CIA or not, Boards should require the performance of a compliance program effectiveness review.

<sup>5</sup> "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 American Health Lawyers Association, page 1 ; para 3.

## About Navigant Consulting

Navigant Consulting, Inc. (NYSE:NCI) is a specialized independent consulting firm providing dispute, financial, regulatory and operational advisory services to government agencies, legal counsel and large companies facing the challenges of uncertainty, risk, distress and significant change. We focus on industries undergoing substantial regulatory or structural change including healthcare, financial services, insurance, energy and on the issues driving these transformations. Navigant Consulting is an international firm with over 1,800 professionals in cities across North America, Europe and Asia.

### Contact »

Bernard J. Ford  
312.583.5765  
bjford@navigantconsulting.com

Saul B. Helman, M.D.  
312.583.3741  
saul.helman@navigantconsulting.com

Geoffrey Kaiser, Esq.  
646.227.4212  
jeff.kaiser@navigantconsulting.com

Carol Landsman  
609.219.8713  
carol.landsman@navigantconsulting.com

David Yarin  
781.270.8305  
dyarin@navigantconsulting.com

Urszula Zapolska  
312.583.4114  
urszula.zapolska@navigantconsulting.com

[www.navigantconsulting.com](http://www.navigantconsulting.com)

Dr. Floyd Loop, a Tenet Healthcare Corporation Board Director and Chairman of Tenet's Quality, Compliance & Ethics Committee, believes that healthcare organizations must be more proactive regarding compliance: "In the new world of increased regulations and surveillance, organizations must integrate compliance into governance before something bad happens. This starts with having a compliance officer who reports to the Board and not to the general counsel, and provides regular updates to the Board about compliance activities. An effective compliance program makes an organization's enterprise risk management process easier. The compliance function should have stature within the organization which includes regular communication with operations and finance. Otherwise compliance activity will be reactive to problems rather than a preventive activity."

W. Neil Eggleston, a Partner with Debevoise & Plimpton LLP, advises and serves as legal counsel to the Board of Directors of multiple organizations, including Tenet Healthcare Corporation. According to Mr. Eggleston, one of the key communication strategies for management is to be equally forthcoming about both good news and bad news. "Tell the Board the good news and the bad news. Management may be reluctant to share bad news, but this undervalues the role of the Board. At the same time, management shouldn't try to slip bad news by the Board, but should fully explain the significance of the matter reported. Management may try to satisfy the "We told the Board about it" obligation, but doesn't ex-

plain the matter to identify, for example, the need for immediate investigation or corrective action. In summary, tell the Board the good news, the bad news, and explain it."

## Conclusion

Recent regulatory developments and corporate integrity agreements have required Boards to be accountable for the oversight of an effective compliance program in their organizations. As part of their oversight, it is essential for Boards to receive succinct information from the COO and management regarding key aspects of an effective compliance program (as promulgated by the OIG), along with key industry risk areas and compliance with CIA requirements (if applicable). This information should include implemented or proposed corrective actions to deficiencies noted.

In addition, even if not subject to a CIA requirement, Boards should require the performance of a compliance program effectiveness review, which should also be structured around the seven (7) elements, and include testing steps for certain compliance program activities. The review report should also include corrective action steps for deficiencies or improvement opportunities identified. With reporting to the Board and/or the performance of a compliance program effectiveness review, management should provide the analysis of compliance-related data and information clearly and effectively, without inadvertently delegating a management role to the Board.

©2009 Navigant Consulting, Inc. All rights reserved.

Navigant Consulting is not a certified public accounting firm and does not provide audit, attest, or public accounting services. "NAVIGANT" is a service mark of Navigant International, Inc. Navigant Consulting, Inc. (NCI) is not affiliated, associated, or in any way connected with Navigant International, Inc., and NCI's use of "NAVIGANT" is made under license from Navigant International, Inc. See [www.navigantconsulting.com/licensing](http://www.navigantconsulting.com/licensing) for a complete listing of private investigator licenses.