



Compliance - TODAY

August 2012

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG



Meet Rachel Rusch

Financial Operations

Billing Supervisor

See page 16

20

**Statistical aspects
of Medicare audits**

Theresamarie Mantese,
Gregory M. Nowakowski,
and Allise Wachs

25

**Protecting
VIP patients'
privacy**

Kim E. Greene
and Jeff Scribner

32

**Solving the
Medicaid
secondary
payment puzzle**

Salvatore G. Rotella, Jr.

38

**ERM and evidencing
compliance program
effectiveness**

Cornelia M. Dorfschmid
and Camella Boateng

by Cornelia M. Dorfschmid, PhD and Camella Boateng, MPH, CHC

ERM and evidencing compliance program effectiveness

- » Effective compliance programs must answer three fundamental questions.
- » Effectiveness measurement promotes better tracking and follow-up.
- » COSO ERM includes scoring measures (i.e., probability/impact analysis).
- » ERM is an ongoing process that must include stakeholders at all levels.
- » ERM is intense and requires interdepartmental collaboration to be successful.

Cornelia M. Dorfschmid (cdorfschmid@strategiccm.com) is Executive Vice President and **Camella Boateng** (cboateng@strategiccm.com) is Senior Associate with Strategic Management in Alexandria, VA.

In an era of health care reform and increased scrutiny on health care compliance, providers and suppliers must protect themselves against the heightened policing by federal and state government agencies. The Patient Protection and Affordable Care Act (PPACA), as amended by the Health Care and Education Reconciliation Act of 2010, mandates that health care providers and suppliers adopt a compliance and ethics program as a condition of participation in the Medicare, Medicaid, and Children's Health Insurance programs. Many providers and suppliers, particularly those of larger entities, have already established compliance programs and thus, the PPACA provisions regarding mandatory compliance programs may not raise immediate concerns. Nonetheless, merely having a compliance program is not sufficient. It must also be effective. In this context of evidencing effectiveness, the case for enterprise risk management (ERM) deserves another look.¹

The adoption of the ERM approach is an effective and productive way to meet and exceed the ever-increasing regulatory demands in today's health care enforcement

environment. ERM not only provides a best practice approach for effective board oversight of the compliance program, but is also a cross-cutting method that identifies, analyzes, controls, mitigates, and monitors an organization's risks. Our brief overview of ERM aims to encourage providers to join the ERM bandwagon, because it not only assists an organization in evidencing an effective compliance program, but also may be the best tool to survive and thrive in the current regulatory environment.



Dorfschmid



Boateng

What is an effective compliance program?

According to section 8B2.1 of the Federal Sentencing Guidelines and further defined by the Department of Health and Human Services Office of Inspector General (OIG), there are seven elements to an effective compliance program.² The elements are as follows:

1. Establish compliance standards and procedures to deter crime, fraud, and abuse.
2. Provide appropriate oversight of the compliance program. This should involve high-level personnel in the oversight of the compliance program. Notably, high-level

personnel must be knowledgeable about the content and operations of the compliance program and should exercise reasonable oversight of the implementation and effectiveness of the compliance program.

3. Communicate compliance standards and procedures to employees through education and training programs.
4. Establish monitoring and auditing systems to detect criminal conduct. In addition, organizations must periodically evaluate the effectiveness of the compliance program.
5. Develop and publicize a reporting system that allows anonymity or confidentiality when employees report or seek guidance concerning potential or actual compliance violations. Further, employees should be able to report violations without the fear of retaliation.
6. Promote and consistently enforce standards.
7. Respond appropriately to any violations. Corrective actions may require modifying the compliance standards and procedures as well as implementing additional preventative measures.

The Federal Sentencing Guidelines further note an “eighth element” that requires organizations to periodically assess their risk of criminal conduct. The ERM method, as well as tools supporting the method, can assist organizations with assessing and prioritizing their risks of non-compliance related to these elements, and provide the support needed to mitigate identified risks.

What is ERM?

ERM is not a new concept. It is a method that was adopted and practiced by many financial and health care organizations after the enactment of the Sarbanes Oxley Act. The

Committee of Sponsoring Organization of the Treadway Commission (COSO), a voluntary private sector organization that develops frameworks and guidances on enterprise risk management, internal controls, and fraud deterrence, describes ERM as:

“[A] process effected [sic] by the entity’s board of directors, management, and other personnel, applied in a strategy setting and across the enterprise. [It is] designed to identify potential events that may affect the entity and managed risks to be within the risk appetite [of the organization and] to provide reasonable assurance regarding the achievement of objectives.”³

COSO’s ERM method provides the health care industry with a way to assess and manage compliance risks from a multidisciplinary perspective. Under the COSO ERM method, it is understood that risks are not one-dimensional. Rather, a risk area can affect various departments within the organization. For example, if a hospital identified inadequate medical documentation as a risk area, this risk can have a financial, operational, legal, and/or regulatory impact on the organization. Thus, not only are personnel involved in patient care affected by the risk area, but the hospital’s Health Information Management, Coding, Billing, Legal, and Compliance departments are also impacted. Consequently, health care organizations should adopt a risk management methodology that assesses risks across the entire organization. The COSO ERM is a method that health care entities can use to address this.

How does the COSO ERM method work?

Health care entities that implement the COSO ERM method are proactively addressing compliance risks instead of only reacting to compliance violations. More specifically, the

COSO ERM method consists of eight components that are integrated in the organization's management processes. COSO's ERM relies on an event-based risk assessment methodology that lends itself to calculations of financial exposure for the organization. The eight components of the COSO ERM method⁴ are as follows:

1. **Internal environment:** This incorporates the tone of the organization and establishes a basis for how risks are viewed and assessed by the organization. This includes the organization's risk management philosophy, risk appetite, and integrity and ethical values.
2. **Objective setting:** The organization establishes objectives before identifying potential events affecting its overall goals. This component of COSO ERM ensures that the organization has a process to establish objectives and that the selected objectives support and align with the organization's mission and risk appetite.
3. **Event identification:** Internal and external events affecting the organization's ability to meet its objectives are identified. The identified events are distinguished between risks and opportunities. Opportunities are channeled back to the organization's strategy or objective setting processes. Identified risk events are further evaluated via a risk assessment.
4. **Risk assessment:** The organization evaluates the risks by assessing the probability and impact of the risk occurring. This process will help organization to determine how the risk should be managed.
5. **Risk response:** The organization selects risk responses and develops corrective actions to align the risk with the organization's risk tolerance and appetite.
6. **Control activities:** The organization establishes and implements policies and procedures to facilitate effective execution of risk responses.
7. **Information and communication:** Involves identifying, capturing, and communicating relevant information in a manner and timeframe that allows personnel to carry out their responsibilities.
8. **Monitoring:** The organization monitors its risk management processes and makes modifications when necessary.

Every compliance officer should be familiar with the basic aspects of ERM methods, such as COSO, and explore how the methods can be integrated with already ongoing risk management efforts in operations. Efforts can begin with assembling a risk universe that organizes risk areas for purposes of risk identification. Risk areas can come from the Centers for Medicare & Medicaid Services contractor (e.g., Recovery Audit Contractors) Work Plans, OIG Work Plans, New York State Office of the Medicaid Inspector General's (OMIG's) Work Plans, OIG Compliance Program Guidances (CPGs), entity-internal sources, etc.

Risk assessment and risk exposure calculations can use simple probability and impact scoring that relies on high (H), medium (M), low (L), or a combination of numerical and qualitative scores, such as H=3, M=2, and L=1. Risk prioritization and ranking that lead to risk response and control activities can be made more transparent using this method. Documents created following the COSO ERM method will undoubtedly support the efforts of an effective compliance program.

Why have effective compliance programs?

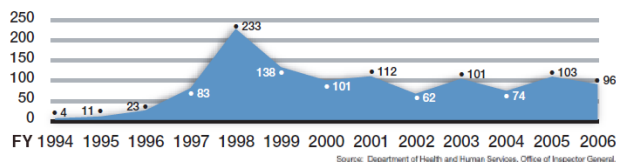
An effective compliance program plays a critical role in reducing an organization's overall exposure to fraud and abuse. Both federal and state regulatory agencies are becoming more aggressive in their fraud and abuse enforcement initiatives. In addition, increased investigative resources provided

under PPACA to federal and state regulators have strengthened the government’s ability to detect fraud and abuse. As a result, more providers are undergoing federal and state audits and investigations—and reaching settlements.

Since 1994, OIG has entered into more than 1,000 corporate integrity agreements (CIAs) with a variety of entities to settle civil fraud allegations and avoid exclusion from participating in health care programs (see Graph 1).⁵ A number of historic high-dollar settlements have occurred,⁶ such as Pfizer’s \$2.3 billion settlement, the largest health care fraud settlement in US history,⁷ and Health Alliance of Greater Cincinnati and Christ Hospital’s \$108 million settlement, which marks the largest settlement ever imposed on a single hospital for allegedly violating the Anti-Kickback Statute.⁸

Entering into a CIA is expensive and time consuming. CIAs not only require a substantial amount of staff resources, but also, among other requirements outlined in a CIA, require an organization to adopt policies and procedures, and conduct training and auditing and monitoring activities to ensure that the organization maintains an effective compliance program.

Another noteworthy reason that highlights the importance of establishing an effective compliance program is the practice of mandated certification of compliance program effectiveness. Under New York state law, Medicaid providers must annually certify that their organizations have effective compliance programs. In the OMIG’s Work Plan for 2012, the Office will follow up with providers who have not certified. Additionally, OMIG may require documentary evidence related to compliance vulnerabilities and activities. This is an important point, because other state Medicaid offices may follow similar practices. Further, the federal government may also conduct audits on compliance program effectiveness in



Graph 1:
Number of Corporate Integrity Agreements Executed by OIG⁵

the future, due to the PPACA provisions that mandate compliance programs.

Generally, it is more cost effective to be proactive and preventive than to face government audits and serious investigations. In the Department of Justice’s (DOJ) revised Principles of Federal Prosecution of Business Organizations, it states that there are “no formulaic requirements regarding corporate compliance programs.”⁹ However, the DOJ does provide three fundamental questions that any prosecutor would ask of an effective program:

- ▶ Is the corporation’s compliance program well designed?
- ▶ Is the program being applied earnestly and in good faith?
- ▶ Does the corporation’s compliance program work?

Organizations must be able to answer these same questions favorably. Providers and suppliers should assess their ability to evidence that their compliance programs are actually working in the event of federal government audits or investigations. It is important to note that although compliance risks can never be fully controlled and avoided, providers must demonstrate that the risks have been mitigated. In addition, a reasonable risk posture (i.e., any calculated risks accepted by an organization and consistent with its size and complexities) is part of doing business while being in compliance with laws and regulations. Overall, the ERM method can support and provide evidence for all three DOJ questions.

Where to go from here?

Providers and suppliers must seriously assess their compliance programs and how their organizations intend to evidence the programs' effectiveness. The ERM approach can address variety of compliance concerns, including providing evidence of an effective compliance program. Compliance officers should give the ERM another look. ☐

1. Peregrine, Michael W: "ERM— It's BAAACK! Fiduciary Duty and Enterprise Risk Management." American Health Lawyer Association, *Connections*, June 2010: 34-38
2. Dowell, Michael A: "New Federal Sentencing Guidelines requirements for an effective compliance program." Health Care Compliance Association, *Compliance Today*, September 2010, pp 32-47
3. Committee of Sponsoring Organizations of the Treadway Commission: "Effective Enterprise Risk Oversight: The Role of the Board of Directors." 2009. Available at: http://www.coso.org/documents/COSOBoardsERM4pager-FINALRELEASEVERSION82409_001.pdf
4. Committee of Sponsoring Organizations of the Treadway Commission: "Enterprise Risk Management — Integrated Framework Executive Summary." 2004. Available at: http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf
5. Department of Health and Human Services Office of the Inspector General: "Protecting Public Health and Human Services Programs: A 30-Year Retrospective." 2006. Available at: <http://oig.hhs.gov/publications/docs/retrospective/AnniversaryPub.pdf>
6. Department of Justice Office of Public Affairs: "Department of Justice Recovers \$3 Billion in False Claims Cases in Fiscal Year 2010." *Justice News*, Nov 22, 2010. Available at: <http://www.justice.gov/opa/pr/2010/November/10-civ-1335.html>
7. Department of Justice Press Release: "Justice Department Announces Largest Health Care Fraud Settlement in Its History: Pfizer to pay \$2.3 Billion for fraudulent marketing." Sept 2, 2009. Available at: <http://www.hhs.gov/news/press/2009pres/09/20090902a.html>
8. Department of Justice Press Release: "The Health Alliance of Greater Cincinnati and the Christ Hospital to Pay \$108 Million for Violating Anti-Kickback Statute and Defrauding Medicare and Medicaid." May 21, 2010. Available at: <http://www.justice.gov/opa/pr/2010/May/10-civ-602.html>
9. Department of Justice: "Corporate Charging Guidelines for Prosecuting Corporate Fraud." 2008. Available at: <http://www.justice.gov/opa/documents/corp-charging-guidelines.pdf>

Start planning now for HCCA's upcoming

2012 Regional Conferences

HCCA's regional, one-day conferences provide **high-quality, convenient, inexpensive education & networking opportunities.**

Don't miss the opportunity to attend one in your area!



New England — September 7 | Boston, MA

Upper Midwest — September 14 | Minneapolis, MN

Midwest — September 21 | Overland Park, KS

North Central — October 5 | Indianapolis, IN

East Central — October 12 | Pittsburgh, PA

Hawaii — October 19 | Honolulu, HI

Mountain — October 26 | Denver, CO

Mid Central — November 9 | Louisville, KY

Desert Southwest — November 16 | Phoenix, AZ

South Central — November 30 | Nashville, TN

New Upper West Coast — December 7 | Oakland, CA

Learn more & register at
www.hcca-info.org/regionals