NYSARC/CP Compliance Seminar: Risk Assessments

May 2, 2016

Robert Hussar and Melissa Zambri

rhussar@barclaydamon.com

mzambri@barclaydamon.com

BARCLAY DAMON LLP

Agenda

- Introductions
- Compliance Risk Assessment Process
- OMIG Effectiveness Review Guidance
- Federal Guidance
- COSO Standards
- NYSARC Chapter Template Risk: Compliance Assessment Policy and Procedures

Federal Government Activity in 2016

- Recovered $3.3 billion associated with health care fraud
- HHS-OIG
  - Investigations resulted in 765 criminal actions and 690 civil actions.
- DOJ:
  - Opened 975 new criminal health care fraud investigations and 930 new civil health care fraud investigations.

OMIG's Guidance & Risk Assessments: Element 6

- 18 NYCRR 521.3 (c)(6)
  - A required provider's compliance program shall include the following elements:
    - (6) a system for routine identification of compliance risk areas specific to the provider type, for self-evaluation of such risk areas, including but not limited to internal audits and as appropriate external audits, and for evaluation of potential or actual non-compliance as a result of such self-evaluations and audits, credentialing of providers and persons associated with providers, mandatory reporting, governance, and quality of care of medical assistance program beneficiaries;

Element 6: Assessments

- A system in effect for . . .
  - 6.1: Routine identification of compliance risk areas specific to your provider
    - Evidence of system:
      - Self-assessment tool
      - Compliance work plan
      - System operating on a regular basis
      - List of identified compliance risk areas
        - » E.g., Medicaid billings/payments, credentials
    - Risk Identification must focus on the type of provider
  - 6.2: Self-evaluation of the risk areas identified in 6.1
    - Internal and external audits (as appropriate)
    - There must be a system for self-evaluations of the risk areas:
      - Examples of evidence include: Written expectation for routine self-evaluations of identified risk areas, and documented results of self-evaluations and work plan activities

Element 6: Assessments Cont.

- 6.3: Evaluation of potential or actual non-compliance as a result of audits and self-evaluations
  - A system for evaluation of potential or actual non-compliance as a result of audits and self-evaluations identified in 6.2
  - Evidence of a system:
    - When self-evaluations and audits of compliance risk areas identified in 6.1 are conducted by individuals outside the compliance function - the results should be shared with the compliance function.
    - Risks are prioritized – identify frequency and impact
    - A compliance work plan that identifies evaluation of potential or actual non-compliance as a result of audits and self-evaluations identified in 6.2
    - Documented results of:
      - » Work plan activities
      - » Root cause analysis of potential or actual non-compliance as a result of audits and self-evaluations identified in 6.2

Element 6: Additional Considerations

- Written descriptions are the best evidence of a system.
- But … if there are not any written descriptions, then evidence of a system may include:
  - Verbal descriptions, demonstrations of the system, or descriptions included in training materials, and
  - Evidence of the outcome of the system's operation
    - Report logs, work plans, documentation and reports of audits, plans of correction.
  - Evidence of appropriate responses related to reports, resolutions, preparation, and distribution of compliance issues.

Risk Assessment Overview:

- Identification of Risk
- Measure/Prioritize the Risk
- Assess the Risk
- Respond to the Risk

Compliance Risk Assessment: Process

- Identify all possible risks in a given area
  - E.g., documentation issues, referral sources, HIPAA
- Analyze and evaluate high-risk areas
  - Consider the changing regulatory environment
- Risk remediation work plan
  - Start with the highest risk areas and evaluate internal controls
- Risk monitoring and auditing
  - On-going process
  - Decide whether to use an inside or outside entity to audit
- Risk Reporting
  - Keep board members and executives informed
  - If fraud is identified, consult counsel to handling government notifications

Compliance Risk Assessment

- **Determine the scope of compliance risks to be assessed**
  - Make an initial list of compliance risks
    - E.g., using an excluded physician, employee credentialing,; submitting a claim to a government payor for a service not performed
- **Identify your organization's key compliance risk-related data**
  - Areas to consider for collecting data:
    - External reviews
    - Strategic plans
    - OIG/OMIG Annual Work Plan related initiatives
    - Billing claims denials by department
- **Finalize set of risks to be assessed**
  - Solicit input and review risk-related data and information gathered
  - Interview employees in key compliance-related areas

Compliance Risk Assessment

- **Evaluate control activities and levels of risk mitigation**
  - Use a risk management committee to evaluate the risk information and control activities.
- **Calculate risk concern levels and rank risk areas**
  - Evaluate subjective and objective measures to determine level of risk.
- **Confirm risk evaluations results with senior management and compliance committee**
  - Present and discuss results of risk evaluation with the compliance committee and senior executives.

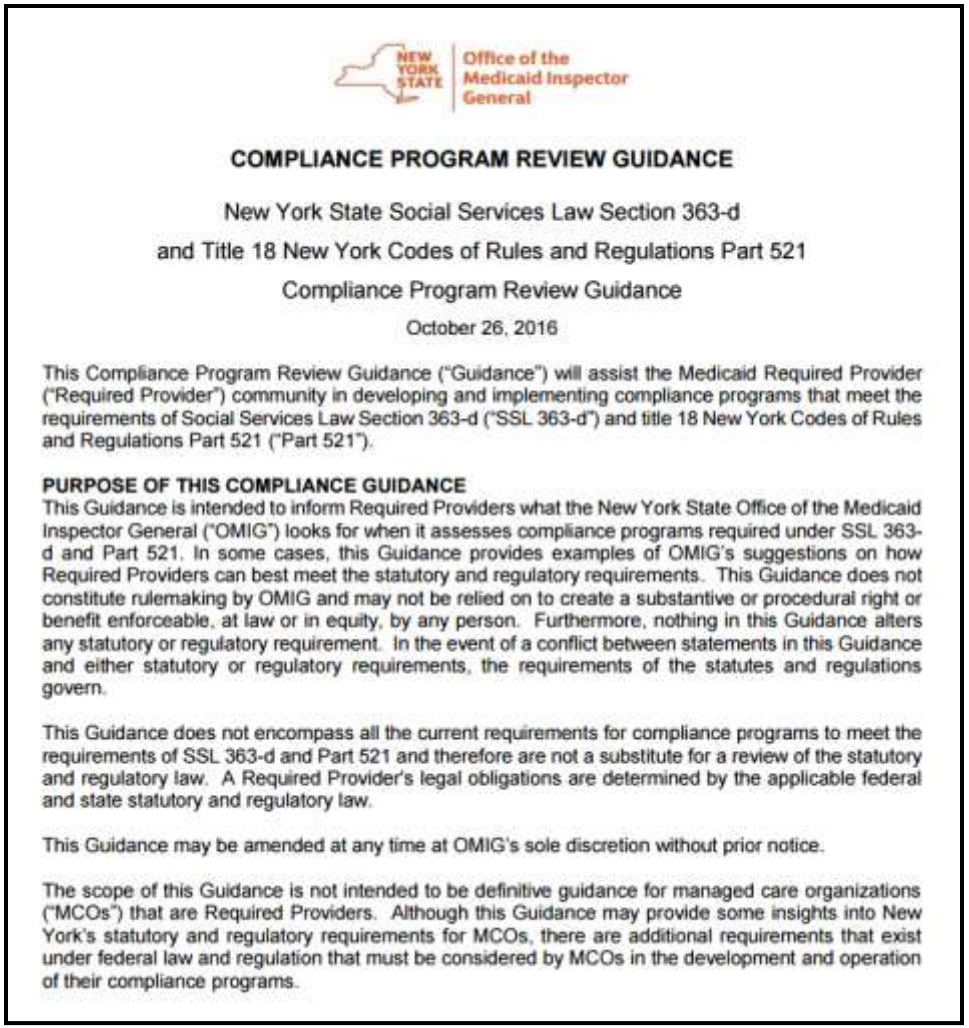
Compliance Risk Assessment

- **Prepare a performance improvement action plan**
  - Assign responsibilities and timelines for plan
- **Review compliance risk assessment results with board members**
  - Ensure the board committee overseeing compliance issues is educated on the compliance risk assessment process followed by the organization
- **Incorporate risk assessment results into compliance work plan and internal audit planning**

Compliance Risk Assessment

- A compliance program should reflect a provider's size, complexity, resources, and culture.
- Analyze the required eight elements.

OMIG Effectiveness Reviews



NEW YORK STATE | Office of the Medicaid Inspector General

COMPLIANCE PROGRAM REVIEW GUIDANCE

New York State Social Services Law Section 363-d

and Title 18 New York Codes of Rules and Regulations Part 521

Compliance Program Review Guidance

October 26, 2016

This Compliance Program Review Guidance ("Guidance") will assist the Medicaid Required Provider ("Required Provider") community in developing and implementing compliance programs that meet the requirements of Social Services Law Section 363-d ("SSL 363-d") and title 18 New York Codes of Rules and Regulations Part 521 ("Part 521").

PURPOSE OF THIS COMPLIANCE GUIDANCE

This Guidance is intended to inform Required Providers what the New York State Office of the Medicaid Inspector General ("OMIG") looks for when it assesses compliance programs required under SSL 363-d and Part 521. In some cases, this Guidance provides examples of OMIG's suggestions on how Required Providers can best meet the statutory and regulatory requirements. This Guidance does not constitute rulemaking by OMIG and may not be relied on to create a substantive or procedural right or benefit enforceable, at law or in equity, by any person. Furthermore, nothing in this Guidance alters any statutory or regulatory requirement. In the event of a conflict between statements in this Guidance and either statutory or regulatory requirements, the requirements of the statutes and regulations govern.

This Guidance does not encompass all the current requirements for compliance programs to meet the requirements of SSL 363-d and Part 521 and therefore are not a substitute for a review of the statutory and regulatory law. A Required Provider's legal obligations are determined by the applicable federal and state statutory and regulatory law.

This Guidance may be amended at any time at OMIG's sole discretion without prior notice.

The scope of this Guidance is not intended to be definitive guidance for managed care organizations ("MCOs") that are Required Providers. Although this Guidance may provide some insights into New York's statutory and regulatory requirements for MCOs, there are additional requirements that exist under federal law and regulation that must be considered by MCOs in the development and operation of their compliance programs.

OMIG: Compliance Program Review Guidance

- **General Requirements**
  - To meet the requirements under the law, a compliance program must:
    - Be appropriate to the Required Provider's characteristic;
    - Apply to "All affected individuals"
    - Meet all the requirements of each of the Eight Elements;
    - Apply to each of the Seven Areas;
    - Be implemented; and
    - Produce results that can be reasonably expected of an operating compliance program that meets the Eight Elements and applies to the Seven Areas.

OMIG: Compliance Program Review Guidance

- **The Eight Elements:**
  1. Written policies and procedures
  2. Designate an employee vested with responsibility
  3. Training and education
  4. Lines of communication to the responsible compliance position
  5. Disciplinary policies to encourage good faith participation
  6. A system for routine identification of compliance risk areas
  7. A system for responding to compliance issues
  8. A policy of non-intimidation and non-retaliation

OMIG: Compliance Program Review Guidance Cont.

- **Seven Areas**
  - Billings
  - Payments
  - Medical necessity and quality of care
  - Governance
  - Mandatory reporting
  - Credentialing
  - Other risk areas that are or should with due diligence be identified by the provider.

Federal Guidance: OIG and DOJ

- OIG: Measuring Compliance Program Effectiveness: A Resource Guide

- DOJ: Evaluation of Corporation Compliance Programs

HCCA-OIG: Resource Guide

Measuring Compliance Program Effectiveness: A Resource Guide

ISSUE DATE: MARCH 27, 2017

HCCA-OIG Compliance Effectiveness Roundtable
Roundtable Meeting: January 17, 2017 | Washington, DC

Measuring Compliance Program Effectiveness – A Resource Guide

HCCA-OIG Compliance Effectiveness Roundtable
Roundtable Meeting: January 17, 2017
Washington DC

HCCA-OIG Resource Guide: Risk Assessment – Element 5

- Element 5: Monitoring, Auditing, and Internal Reporting Systems
  - Risk Assessments:
    - Documentation/Process Review
  - Other Risk Assessment metrics:
    - Process
    - Risk Based work/audit plan
    - Follow-up
    - Frequency, scope, coverage and tools
    - Information flow from business units to compliance department for risk assessment process
    - Participation of business leadership in risk resolution
    - Documentation/process review
  - Audit and monitor based on risk assessment
  - Random auditing is conducted to identify unknown risks

HCCA-OIG Resource Guide: Risk Assessment – Other Elements

- **Element 1**: Standards, Policies, and Procedures
  - Based on assessed risks
- **Element 2**: Compliance Program Administration
  - Risk assessment Cycle
  - Work Plan development on risk assessment
  - Prioritization of risk consultation with applicable partners (e.g., legal, HR, IT, risk management)
- **Element 4**: Communication, Education, and Training on Compliance Issues
  - The organization:
    - Bases training for individuals who are designated to be in high-risk positions on a formal process for assessing risk and evaluating control vulnerabilities.
    - Develops issue-specific training based on the results of the risk assessment and identified internal control weaknesses.
    - Integrates specific risks identified through the risk assessment process into compliance training.

DOJ: Evaluation of Corporation Compliance Programs

U.S. Department of Justice
Criminal Division
Fraud Section

Evaluation of Corporate Compliance Programs

Introduction

The Principles of Federal Prosecution of Business Organizations in the United States Attorney's Manual describe specific factors that prosecutors should consider in conducting an investigation of a corporate entity, determining whether to bring charges, and negotiating plea or other agreements. These factors, commonly known as the "Filip Factors," include "the existence and effectiveness of the corporation's pre-existing compliance program" and the corporation's remedial efforts "to implement an effective corporate compliance program or to improve an existing one."

Because a corporate compliance program must be evaluated in the specific context of a criminal investigation that triggers the application of the Filip Factors, the Fraud Section does not use any rigid formula to assess the effectiveness of corporate compliance programs. We recognize that each company's risk profile and solutions to reduce its risks warrant particularized evaluation. Accordingly, we make an individualized determination in each case.

There are, however, common questions that we may ask in making an individualized determination. This document provides some important topics and sample questions that the Fraud Section has frequently found relevant in evaluating a corporate compliance program. The topics and questions below form neither a checklist nor a formula. In any particular case, the topics and questions set forth below may not all be relevant, and others may be more salient given the particular facts at issue.

DOJ Evaluation of Corporation Compliance Programs

Risk Assessment

- Risk Management Process:
  - What methodology has the company used to identify, analyze, and address the particular risks it faced?
- Information Gathering and Analysis:
  - What information or metrics has the company collected and used to help detect the type of misconduct in question? How has the information or metrics informed the company's compliance program?
- Manifested Risks:
  - How has the company's risk assessment process accounted for manifested risks?

DOJ Evaluation of Corporation Compliance Programs

Continuous Improvement, Periodic Testing and Review

- **Internal Audit:**
  - What types of audits would have identified issues relevant to the misconduct? Did those audits occur and what were the findings? What types of relevant audit findings and remediation progress have been reported to management and the board on a regular basis? How have management and the board followed up? How often has internal audit generally conducted assessments in high-risk areas?
- **Control Testing:**
  - Has the company reviewed and audited its compliance program in the area relating to the misconduct, including testing of relevant controls, collection and analysis of compliance data, and interviews of employees and third-parties? How are the results reported and action items tracked? What control testing has the company generally undertaken?
- **Evolving Updates:**
  - How often has the company updated its risk assessments and reviewed its compliance policies, procedures, and practices? What steps has the company taken to determine whether policies/procedures/practices make sense for particular business segments/subsidiaries?

COSO

- **C**ommittee of **S**ponsoring **O**rganizations of the Treadway **C**ommission
- Joint initiative of five private sector organizations
  - American Accounting Association
  - American Institute of CPAs
  - Financial Executives International
  - The Association of Accountants and Financial Professionals in Business
  - The Institute of Internal Auditors
- Develops frameworks and guidance:
  - Enterprise risk management
  - Internal controls
  - Fraud deterrence

COSO Standards

- Designed to assess an organization's internal controls
- OPWDD utilizes the COSO framework to evaluate providers' internal controls.
  - Understand a provider's internal controls
  - Identify any areas where there could be improvement

COSO Framework

- The New COSO Internal Control – Integrated Framework Principles (2013)
- Comprised of 5 Internal Control Components and 17 COSO principles.
- Internal Control Components:
  - Control the Environment
  - Risk Assessment
  - Control Activities
  - Information and Communication
  - Monitoring Activities

Internal Control Components for OPWDD Providers

- Internal Control Components:
  - Control the Environment:
    - The overall support by management of the components of internal control.
    - Factors to consider: ethical values, integrity, and operating style.
  - Risk Assessment:
    - Asses the risk in order to manage and minimize the impact of negative events.
  - Control Activities:
    - Adopt policies and procedures
    - Policies and Procedures enable the board to understand their fiduciary responsibilities, manage assets properly, and carry out the charitable purposes of the organization.
  - Information and Communication:
    - Adequate information systems can identify and communicate information in a timely manner.
    - The information should be communicated in a timeframe that enables people to carry out their responsibilities.
  - Monitoring Activities:
    - Continuously monitor and evaluate internal control system's performance.

Applying the COSO Standards to Fraud Risk Management

- Control the environment
  - Principle 1: The organization establishes and communicates a Fraud Risk Management Program that demonstrates the expectations of the board of directors and senior management and their commitment to high integrity and ethical values regarding managing fraud risk.
- Risk assessment
  - Principle 2: The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities and implement actions to mitigate residual fraud risks.

Applying the COSO Standards to Fraud Risk Management Cont.

- Control activities
  - Principle 3: The organization selects, develops, and deploys preventive and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner.
- Information and communication
  - Principle 4: The organization establishes a communication process to obtain information about potential fraud and deploys a coordinate approach to investigation and corrective action to address fraud appropriately and in a timely manner.
- Monitoring activities
  - Principle 5: The organization selects, develops, and performs ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communicates Fraud Risk Management Program deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the board of directors.

OPWDD Audit Findings with COSO Framework

- The need for an integrated control structure for HCBS waiver billings.
- The absence of an Enterprise Risk manager
- A need for written policies and procedures when using software packages.
- Insufficient monitoring
  - Requires internal auditing on HCBS Waiver Services.

NYSARC Chapter Template: Risk Compliance Assessment Policy and Procedures

- **Policy:**
  - Covers the Seven Areas
    - OMIG Compliance Guidance
- **Procedure:**
  - Review CMS, HHS, the Justice Center, OIG, OMIG, and OPWDD information sources to identify areas of compliance work plan focus for next 12 months
  - Consult with other Provider Associations to ascertain compliance risk areas
  - Complete the OMIG “Compliance Program Self-Assessment Form” to identify weaknesses
  - Conduct interviews with key operational and administrative staff
  - Conduct interviews with key governance members
  - Internal Audit Findings: Review results of internal audits to identify areas where problems have been identified
  - Self Disclosures or Claim Voids
  - External Audit Findings

NYSARC Chapter Template Risk Compliance Assessment Policy and Procedures Cont.

- Documentation
  - Compliance risk areas are identified and documented
  - Risks are prioritized

- Format and Record Retention
  - No prescribed format
  - Assessed risk areas clearly documented

QUESTIONS ?? COMMENTS ……

Thank You!

Melissa Zambri, Esq.
(518) 429-4229
mzambri@barclaydamon.com

Robert Hussar, Esq., CHC
(518) 429-4278
rhussar@BarclayDamon.com
www.hccconnections.com