1

25th Annual HCCA Compliance Institute

Session W4E on Wednesday, April 21 @ 3:30 – 4:35 PM (CST)

What is a Compliance Risk Assessment?

The Art & Science of Conducting an Effective Compliance Risk Assessment

1

2

Presenters

Susan Gillin

Branch Chief, Administrative & Civil Remedies Branch, Office of Counsel to the Inspector General

Jeff Driver

Professor of Innovation Science, Risk Management & Privacy
Edson College,
Arizona State University

Betsy Wade

Chief Compliance & Ethics Officer, Corporate Compliance, Signature Healthcare Consulting Services, LLC, Adjunct Faculty, Edson College, Arizona State University

2

3

Learning Objectives

The Ground Rules and OIG Expectations

Susan Gillin

The Seven Elements

Recent OIG Guidance

Basic Risk Assessment Framework

Crafting Risk Assessments for Effectiveness

Jeff Driver

HCCA/SCCE COSO Guidance

ISO 31000

ASHRM ERM Guidance

Boots on the Ground at the Sharp End

Betsy Wade

Policy and Process

Results and Reporting

Document, Document, Document

3

4

The Ground Rules and OIG Expectations: The Seven Elements

Background: Guidance has evolved over time but still based in USSG

A. The Seven Elements

i. Is Risk Assessment the 8th? In the "new day" of compliance, "You get no bonus points for having a compliance program." (Dan Levinson, 2016)

ii. Risk Assessment is the best tool we have for evaluating whether a compliance program is effective. It tests implementation of the seven elements.

4

The Ground Rules and OIG Expectations: Recent OIG Guidance

5

B. Recent Guidance

i. OIG CIA language (updated 2020)

ii. OIG Effectiveness Guide (2017)

iii. DOJ Evaluation of Corporate Compliance Programs (2017; updated 2020; https://www.justice.gov/criminal-fraud/page/file/937501/download)

iv. Older but still relevant guidance for Boards: leadership needs to engage proactively

5

The Ground Rules and OIG Expectations: The Basic Risk Assessment Framework

6

C. Basic Framework of a Risk Assessment (SAM)

i. (S) Structure – questions to assess compliance program structure

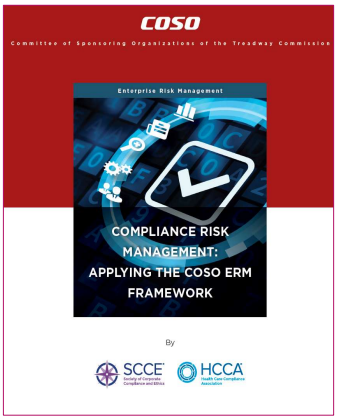
ii. (A) Accountability – questions to assess compliance accountability

iii. (M) Measurement – measure actual implementation and performance of compliance program

6

Crafting Risk Assessments for Effectiveness: SCCE/HCCA COSO Guidance

7



November 11, 2020

COSO releases new guidance, *Compliance Risk Management: Applying the COSO ERM Framework*, detailing the application of the *Enterprise Risk Management—Integrating with Strategy and Performance* (ERM Framework) to the management of compliance risks. The guidance was commissioned by COSO and authored by the Society of Corporate Compliance and Ethics & Health Care Compliance Association (SCCE & HCCA).

See: https://www.coso.org/Documents/Compliance-Risk-Management-Applying-the-COSO-ERM-Framework.pdf

7

Crafting Risk Assessments for Effectiveness: SCCE/HCCA COSO Guidance

8

Source: COSO *Enterprise Risk Management—Integrating with Strategy and Performance*

8

Crafting Risk Assessments for Effectiveness: SCCE/HCCA COSO Guidance

9

Source: *COSO Enterprise Risk Management—Integrating with Strategy and Performance*

9

Crafting Risk Assessments for Effectiveness: ISO 31000 Risk Management Guidance

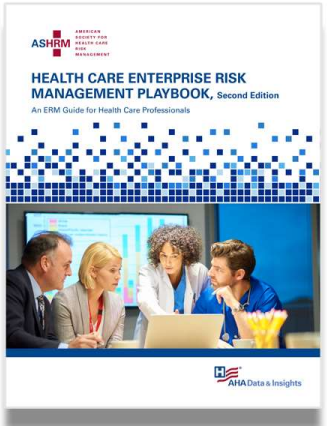
10

https://www.iso.org/iso-31000-risk-management.html

10

Crafting Risk Assessments for Effectiveness: ASHRM ERM Guidance

11



Playbook Description
The ASHRM Enterprise Risk Management, Second Edition serves as a guide to identify opportunities and strategies to advance ERM practices throughout health care organizations and care delivery

Notable Features:
- Crosswalk of COSO Framework and ISO 31000 Guidelines
- Step-by-step guide on how to quantify your risk
- Sample ERM plan and job description
- Includes tools & other ERM resources

https://www.ashrm.org/enterprise-risk-management-playbook-second-edition

11

Crafting Risk Assessments for Effectiveness: ERM Guidance

12

WHAT IS ERM? **It is the capability to effectively answer the following quesions:**

- Circular depiction is highly intentional
- Components are meant to be dynamic (reviewed back/forth in any sequence)
- Having the right culture is key

https://www.rmahq.org/erm-framework/

12

13

Boots on the Ground at the Sharp End: Policy & Process

A. Policy and Process

i. Policy needed to document risk assessment framework/strategy selected
ii. Process can include interviews, document review, surveys, data mining

13

14

Boots on the Ground at the Sharp End: Results & Reporting

B. Results and Reporting

i. Report Risk Assessment results to Compliance Committee and Board
ii. Use Risk Assessment results to update Annual Compliance Plan, and develop Compliance Monitoring Plan and Internal Audit Plan

14

Boots on the Ground at the Sharp End: Document, document, document!

15

C. Document, Document, Document

i. Document action plans and results of monitoring and auditing
ii. Report results to Compliance Committee and Board

15

What would you do? Let's give it go… Let's test out a scenario and learn!

16

The facts

Big Heart Hospital has agreed to pay the U.S. Government $25 million to resolve civil allegations that it submitted false or fraudulent claims to the Medicare and Medicaid programs for a variety of medically unnecessary heart procedures.

Big Heart Hospital also will enter into a Corporate Integrity Agreement with the Department of Health and Human Services, Office of Inspector General ("HHS-OIG"), which obligates the hospital to undertake substantial internal compliance reforms and commit to a third-party review of its claims to federal health care programs for the next five years.

Diagnosis and issues identification

Next slides . . .

The risk assessment, implementation, and the follow-up plan

Next slides . . .

16

17

What would you do? Let's give it a go: Diagnosis and and issues identification

According to the settlement agreement, the U.S. Government contends that from January 1, 2018 until December 31, 2020, several doctors working at Big Heart Hospital performed numerous invasive cardiac procedures on Medicare and Medicaid patients that were not medically necessary. The hospital then billed the federal programs for these unnecessary procedures, which include coronary stents, coronary artery bypass graft surgeries ("CABGS"), and diagnostic catheterizations.

The claims seeking reimbursement allegedly violated the False Claims Act because under federal law, Medicare and Medicaid programs only reimburse health care providers for operations that are deemed medically necessary. Hospitals generally receive between $10,000 and $15,000 for medical procedures such as heart stents.

The doctors were affiliated with a physician group that entered an exclusive arrangement with Big Heart Hospital in 2018 to provide cardiology services to the hospital's patients.

The settlement also resolves allegations that Big Heart Hospital violated the federal Stark Law and Anti-Kickback Statute by entering into sham management agreements with the doctors. These agreements served as an inducement for the doctors to refer patients to Big Heart Hospital. Therefore, the government contends that Medicare and Medicaid are not responsible to pay claims that resulted from this improper financial relationship between the doctors and the hospital.

17

18

What would you do? Let's give it a go: Risk Assessment & The Plan

Assessment of the risk, prioritization, and developing the mitigation plan

- ✓ Billing and coding
- ✓ Medical Necessity
- ✓ Physician contracting and compensation

18

19

What would you do? Let's give it a go: Implementing the mitigation efforts

- ✓ Implementation of policies and procedures, education, hotline, auditing and monitoring, etc.
- ✓ Implementation of risk assessment process and compliance effectiveness review process
- ✓ Internal monitoring and auditing of billing and coding
- ✓ Third-party IRO to test billing and coding
- ✓ External quality review process to monitor medical necessity
- ✓ Third-party IRO to examine quality of care
- ✓ Internal monitoring and auditing of physician transaction process and physician compensation
- ✓ External IRO of physician contracting and compensation

19

20

What would you do? Let's give it a go: The plan for follow-up & communications

- ✓ Annual compliance education employees, physicians and vendors
- ✓ Compliance education for new employees, physicians and vendors
- ✓ Ongoing education around coding and billing, medical necessity, Stark and Anti-kickback, and False Claims
- ✓ Ongoing education on auditing and monitoring results

20

21

OIG Takeaways

Where could providers do better? There needs to be a team approach among leaders of various departments and the Compliance Officer and the General Counsel

OIG CIAs now require this to happen through the Compliance Committee so that we get a cross section of the organization

Where could providers do better? Survey leaders and midlevel managers and ask: what are the risks you see?

This enables you to create a rank order list of risks and decide how many to address (depends on your organization's risk tolerance).

21

22

OIG Takeaways

OIG expects the scope of risk identification to be broad, with room for prioritization of in-depth assessment.

"Within 90 days after the Effective Date, [Provider] shall develop and implement a centralized annual risk assessment and internal review process to identify and address risks associated with [Provider]'s participation in the Federal health care programs, including but not limited to the risks associated with the submission of claims for items and services furnished to Medicare and Medicaid program beneficiaries and the Anti-Kickback Statute and Stark Law risks associated with Arrangements (as defined in Section II.C.1 above). The Compliance Committee shall be responsible for implementation and oversight of the risk assessment and internal review process. The risk assessment and internal review process shall be conducted at least annually and shall require [Provider] to: (1) identify and prioritize risks, (2) develop internal audit work plans related to the identified risk areas, (3) implement the internal audit work plans, (4) develop corrective action plans in response to the results of any internal audits performed, and (5) track the implementation of the corrective action plans in order to assess the effectiveness of such plans. [Provider] shall maintain the risk assessment and internal review process for the term of the CIA."

22

23

OIG Takeaways

OIG continues to encourage the use of data to inform identification of risks.

- ✓ Internal claims data (compare year over year? Look for outlier billers? Most frequent codes billed?)
- ✓ Any external data about how peer organizations are billing those codes
- ✓ OIG reports are also data: audits, evaluations, and case settlements.

23

24

Scholarly Takeaways

Risk assessments are a cornerstone of an effective compliance program and the process should be continuously improved utilizing best available evidence and scientific tools.

- ✓ Adopt, chisel, customize or design a hybrid RA process for periodic, continuous, and focused RA.
- ✓ Forge a continuous plan to foster a proper organizational risk culture and RA alignment with corporate strategy.
- ✓ Understand and periodically assess organizational, board, and executive risk appetite and tolerance levels.
- ✓ Craft subjective risk estimates towards semi-quantitative estimates with proper independent organizational facilitation and heuristic bias controls.
- ✓ With RA maturity consider adding decision science, ROR, and the upside of risk principles to supercharge risk response.
- ✓ Monitor progress and compliance KPI's.

24

25

Practitioner Takeaways

Risk assessments are not optional and should be conducted annually at a minimum.

- ✓ Select a framework for the size and complexity of your organization.
- ✓ Establish a policy and process and follow it.
- ✓ Use your risk assessment results to develop your work plans.
- ✓ Report your results to your Compliance Committee and Board.
- ✓ Test your action plans and adjust as necessary.
- ✓ Document all of your efforts.

25

26

25th Annual HCCA Compliance Institute
Session W4E on Wednesday, April 21 @ 3:30 – 4:35 PM (CST)

What is a Compliance Risk Assessment?
The Art & Science of Conducting an Effective Compliance Risk Assessment

26