Audit & Compliance Committee Board of Directors

Shawn DeGroot, CHC-F, CCEP, CHRC, CHPC
Compliance Vitals

Objectives

- Key areas of consideration in developing and implementing a compliance program
- Risk areas for consideration by the board
- Steps a board may take in considering management accountability related to compliance risks

Compliance Program Foundation

- Policies and Procedures:
  - Orientation to program
  - Development or review
  - Adherence and effectiveness

Compliance Program Foundation

Education

- Compliance and Ethics
- Job-specific educational programs
- Ethics scenario discussions in staff meetings
- Background checks, exclusion checks

Compliance Program Foundation

High level oversight:

- Board
- Senior management participating in meetings
- Exit conferences and interviews
- Compliance Committee meetings
- Compliance Officer member of Senior Management

Risk

Italian for “risicare”:
To dare, a choice under uncertain conditions

International Organization for Standardization (ISO)
The effect of uncertainty on objectives

Webster’s: Possibility of a loss or injury

Risk Assessment vs. Management

- Risk Assessment: Identification, assessment and estimation of risk levels
- Risk Management: Identification, assessment and prioritization based on economical application of resources to control the impact

Organizational Risk Tolerance

- Vision, Values, Mission and Culture drive risk tolerance
- Risk Appetite:
  - Human
  - Natural
  - Environmental

Appetite for Risk

Risk of Driving vs. Flying

A typical domestic flight (694 miles) is as dangerous as driving how many miles in a car on rural interstate highway?

Audit & Compliance Risk Report

- Risk Likelihood
  - High: Expected to occur
  - Medium: Will probably occur
  - Low: May occur at some time in the next # years
- Risk Impact (Severity)
  - High: Serious impact on operations, reputation or funding status
  - Medium Significant impact …
  - Low: Less significant impact …

Risk Report for the Board

		A	B	C	D	E
		Negligible	Minor	Moderate	Significant	Severe
E	Very Likely	Low Med	Medium	Med Hi	High	High
D	Likely	Low	Low Med	Medium	Med Hi	High
C	Possible	Low	Low Med	Medium	Med Hi	Med Hi
B	Unlikely	Low	Low Med	Low Med	Medium	Med Hi
A	Very Unlikely	Low	Low	Low Med	Medium	Medium

Audit & Compliance Risk Report to BOD

- Prioritize: Low, medium, high
  - Identify assets by threats, vulnerability, impact and likelihood
  - Review existing controls, e.g. (how well is the risk managed)
  - Identify risks that will happen but are well-controlled

Audit & Compliance Risk Report

- Manage Results (ERM Framework)
  - Avoidance: exit the activity that creates the high risk
  - Reduction: take action to reduce the likelihood and/or impact
  - Share or insure: transfer/share a portion of the risk
  - Accept: no action is taken, due to a cost/benefit decision

Common Risk Areas:

- Anti-trust
- Board responsibility
- Employment:
  - Labor Laws, wage and hour, breaks
  - Unions
- False Claims Act
- General Data Protection Act

Common Risk Areas:

- Hotlines
- State and Federal Privacy Laws
- Whistleblower Laws
- Transparency
- Background checks
- Quality of data

Common Risk Areas: Privacy & Data Security

- PII and PHI
- State and federal levels
  - Ransomware
  - Password sharing
  - Unencrypted data, devices, drives
  - Snooping/unauthorized data access
  - Security, firewalls, physical security, technical security intrusion detection

Common Risk Areas: Privacy & Data Security

- Social media comments/posts
- Failure to timely report a data breach
- Penalties
- Reputation capital

Poneman Institute 2018

Interviews:
2,200 IT, Data and Compliance Professionals

477 Companies that experienced a data breach in the past 12 months

Risk Mitigation

- Mean time to identify the breach was 197 days
- Mean time to contain was 69 days
- State and federal reporting requirements
- Companies that contained a breach in less than 30 days saved over $1 million
  - Mitigation efforts: Incident response team

Risk Areas: Tax exemption and State Tax

- Federal, state and local government agencies, consumer groups
- Unions and press
  - Charity care ad community benefit
  - Pricing
  - Collection activities
  - Executive compensation and benefits
- State Laws for Internet Sales

Unique Risk Areas: Healthcare

- Anti-kickback and Stark
  - Purpose of the laws are to prevent payment/incentives to physicians designed to induce referrals or impact clinical judgment
  - Risk area for both hospital, individual employees and board
  - Basic Rules: Never offer of anything of value to induce referrals
  - Never pay/rent to or accept rent from a practicing physician without a signed, written agreement
  - Board: education and knowledge

Unique Risk Areas: Healthcare

- Anti-kickback and Stark
  - Written and signed agreement
  - Minimum term of one-year
  - Fair market value compensation/payment
  - Compensation set in advance
  - Must not take into account value or volume of referrals

Unique Risk Areas: Healthcare

Incorrect Claims

- Deliver, code and bill services consistent with law
- Government resources for RAC's, ZPIC's, MAC's, MIC's, etc.
- Claim accuracy rests on revenue cycle function and chargemaster
- Reliance on physician documentation, e.g. medical necessity
- Technical billing requirements (thousands)
- State conditions of participation
- State Medicaid Fraud Control Units

Risk Area Quality

- Transparency: Public reporting of hospital and physician data
  - Bad data
  - Good data
  - Payment is tied to quality
  - Risk exposure – physicians, hospital, management and BOD

Risk Area Quality

- Consistent adherence to Standard of care/protocols
- Avoiding "never events", wrong-site surgeries and Hospital-acquired infections
- "Conditions of Participation Compliance

"Public" reporting of quality data by physician and department will improve results. Transparency changes behavior!

Risk Area Quality

- Credentialing and re-credentialing
- Effective peer review
  - Prompt, independent investigation
  - Comprehensive documentation
  - Corrective action
  - Monitoring corrective action plans
  - Consistent, transparent Board reporting

Government Agencies

- U. S. Federal Sentencing Guidelines for Organizations (FSG)
  - "Organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement to reduce the risk of criminal conduct indentified through its process" §8B2.1 (b)(1)(5)
- HHS OIG Compliance Program Guidance
- OCR, SEC, DOJ, DOL, DOE, FTC

Government Agencies

- Federal Energy Regulatory Commission:
  - Risk Informed Decision-Making Guidelines 2016
  - https://ferc.gov/industries/hydropower/safety/guidelines/ridm/risk-guide/chapter-2.pdf
- Office of Civil Rights
  - All covered entities including small providers, must conduct a “Risk Analysis”
  - Security Rule §164.308(A)(1)

Board of Directors

Understand Risk Management

- Leadership and Organizational support
- Risk identification process
  - Documentation of findings
  - Risk prioritization
- Risk mitigation and corrective action
- Audit and monitor

Risk Review: Questions for the Board

- Is management handling the compliance risk?
- Are the right people and the right culture in place?
- If problems are identified by employees, will they be reported and action taken?
- Is there a reasonable level of assurance that the company is compliant with applicable standards and regulations of its industry?
- Are recurring issues being reported?

Board Responsibilities: Risk

- Risk responsibilities will vary organization to organization; however should be outlined in the Committee Charter
- Quarterly updates on:
  - Policy changes and possibly the "why"
  - Training status
  - Investigations and associated corrective action
  - Violations

Board Responsibilities: Risk

- Review Internal Audit Work Plan, ensure both compliance and operational risks addressed
  - Not all compliance risks are significant enough to be on audit plan
- Review Compliance Work Plan, ensure identified high risks are prioritized and monitored
- International Organization for Standardization: Identify gaps against published standards

Shawn@Compliancevitals.com