Enterprise Risk Management

Kenya Woodruff

Katten Muchin Rosenman LLP

Partner

Agenda

- Joint Commission Standards
- Conditions of Participation
- Elements of Effective Compliance Program
- Practical Compliance Guide for Health Care Governing Boards
- Oversight and Enforcement
- Enterprise Risk Management

Selected Joint Commission Standards

Standard	Requirement
LD.01.03.01	The governing body is ultimately accountable for the safety and quality of care, treatment, and services.
LD 04.01.01	The hospital complies with law and regulation.
LD 04.03.07	Variances in staff, setting, or payment source do not affect outcomes of care, treatment, and services in a negative way.
LD 04.03.09	Care, treatment, and services provided through contractual agreement are provided safely and effectively.

Selected CMS Conditions of Participation

COP (42 CFR)	Elements of Performance
482.12	The hospital must have a governing body which is effective in carrying out its responsibilities for the conduct of the hospital. The governing body must be functioning effectively and holds the ultimate responsibility for the hospital's compliance not only with the specific standards of the governing body CoP, but also with all of the CoPs.
482.12(e)(1) 482.21(e)(4)	The governing body provides for the resources needed to maintain safe, quality care, treatment, and services.
482.11(a) 482.12(d)(5)	The hospital provides care, treatment, and services in accordance with licensure requirements, laws, and rules and regulations.
482.51	Patients with comparable needs receive the same standard of care, treatment, and services throughout the hospital.
482.12(e) 482.12(e)(2)	The hospital describes, in writing, the nature and scope of services provided through contractual agreements.

Elements of Effective Compliance Program

The Seven Fundamental Elements of an Effective Compliance Program

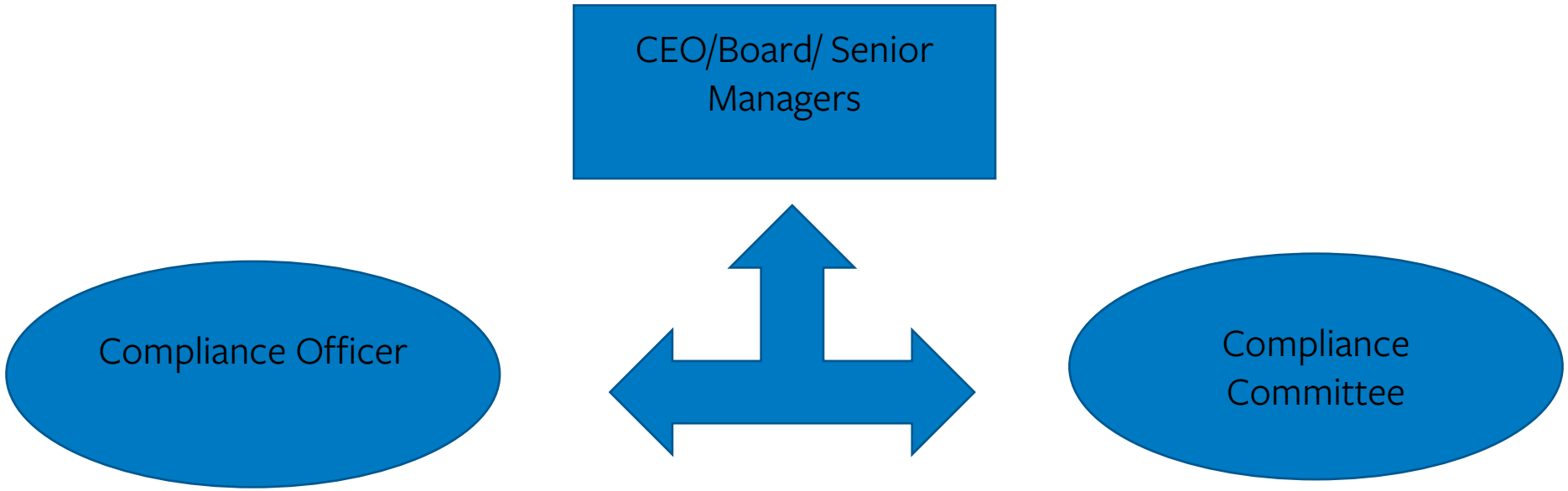
1. Implementing written policies, procedures and standards of conduct
2. Designating a compliance officer and compliance committee
3. Conducting effective training and education
4. Developing effective lines of communication
5. Conducting internal monitoring and auditing
6. Enforcing standards through well-publicized disciplinary guidelines
7. Responding promptly to detected offenses and undertaking corrective action

Written Policies, Procedures, and Standards of Conduct

- Should be unambiguous with detailed expectations
- Made available to all employees
- Frequently updated
- Reviewed by all new hires within 90 days of employment and by current employees annually
- Detailed standards of conduct and means of reporting violations
- Policies should include the role and responsibilities of compliance staff
- Procedures should include training plans and operational details of the program, and interactions with other departments

Designating a Compliance Officer and Compliance Committee

- The Compliance Officer and/or Compliance Committee is responsible for the supervision of the compliance program, and reports directly to the CEO.



Designating a Compliance Officer and Compliance Committee

Compliance Officer/Compliance Committee Duties:

- Developing and implementing procedures for the compliance program
- Enforcing disciplinary standards
- Implementing a system for the assessment of risks
- Reviewing auditing and monitoring reports
- Monitoring the effectiveness of corrective actions
- Coordinating with Human Resources
- Developing an auditing work plan

Conducting Effective Training and Education

- Annual general compliance training for all employees
- Preliminary compliance training for all new hires
- Compliance training should be updated annually to reflect new developments
- Trainings should incorporate real world compliance and non-compliance scenarios to simulate potential risks employees may encounter
- Make trainings interactive to increase employee engagement by “Gamifying” modules, hosting computer based trainings, and offering incentives

Developing Effective Lines of Communication

- There should be requirements for employees to report issues in a timely manner
- Resources for anonymous reporting such as a hotline should be made available to employees

What to communicate:

- Compliance issues and illegal behavior

Who to report compliance issues to:

- The Compliance Officer or Committee
- Assigned Manager/Supervisor

Developing Effective Lines of Communication

How to report compliance issues:

- Face-to-face
- Via email or intranet form
- Anonymously via hotline

When to report compliance issues:

- Immediately or as soon as they are brought to your attention

Conducting Internal Auditing and Monitoring

An effective auditing and monitoring system allows the organization to:

- Measure the impact of the compliance program
- Ensure adherence to the CMS program
- Identify compliance risks

Auditing and Monitoring:

- The auditing and monitoring system should include both internal and external monitoring and audits

Conducting Internal Auditing and Monitoring

Monitoring Functions:

- Occurs regularly (daily, weekly, monthly) throughout normal operations
- Confirms whether procedures are beneficial
- Ensures recommendations and corrective action plans are being implemented
- Performed by staff

Conducting Internal Auditing and Monitoring

Auditing Functions:

- Ensures compliance with CMS and statutory requirements
- Occurs annually, or more frequently, as necessary
- Includes written reports of findings, recommendations, and proposed corrective actions
- Includes periodic evaluations to assess the effectiveness of the compliance program

Enforcement through Well-publicized Disciplinary Guidelines

Written policies should include appropriate disciplinary sanctions for those who violate applicable requirements and standards of conduct

Sanctions should be applied for:

- Non-compliance
- Failure to report actual or suspected non-compliance
- Failure to report non-compliance when non-compliance was evident after due diligence was conducted

Enforcement through Well-publicized Disciplinary Guidelines

Disciplinary policies must:

- Be consistent and taken within a timely manner
- Be unambiguous and well-publicized
- Outline expectations and consequences for non-compliance and unethical and illegal behavior
- Be frequently reviewed with staff

Responding to Detected Offenses and Undertaking Corrective Action

When non-conformances are identified, corrective actions must be taken in response to potential violations

Examples of Corrective Actions Include:

- Repayment of overpayments
- Disciplinary action against responsible employees

Practical Compliance Guide for Health Care Governing Boards

Board Oversight of Compliance Program Functions

- Boards must act in good faith when exercising its oversight responsibility for the organization by ensuring: (1) a corporate information and reporting system exists and (2) the reporting system is reliable
- Boards are encouraged to use widely recognized public compliance resources as benchmarks for their organization such as:
  - The Federal Sentencing Guidelines (Guidelines)
  - OIG's Voluntary Compliance Program Guidance documents
  - OIG's Corporate Integrity Agreements (CIAs)
- Ensuring that management is aware of the guidelines, compliance program guidance, and relevant CIAs plays an important role in ensuring the adequacy of existing compliance systems and functions

Board Oversight of Compliance Program Functions

- The extent and adequacy of the compliance program in relation to the size and complexity of the organization is important for the Board members of health care organizations to assess
- The Guidelines allow for alterations according to the size of the organization
- The government allows smaller organizations to meet the Guidelines requirements with less formality and fewer resources
- Smaller organizations may use available personnel to carry out their compliance and ethics programs

Board Oversight of Compliance Program Functions

- Board members of small organizations should model its compliance and ethics programs to that of similar organizations
- Boards should structure a formal plan to stay informed about changes in the regulatory and operating environments
- Board members should also consider external educational resources to acquire an in-depth understanding of industry risks, regulatory requirements, and additional beneficial compliance and ethics programs

Board Oversight of Compliance Program Functions

- A board can expand its substantive expertise with respect to regulatory and compliance matters by consulting or including on the board a regulatory, compliance, or legal expert
- OIG may require entities under a CIA to consult an expert regarding compliance or governance issues to help the board fulfill its responsibilities under the CIA

Roles and Relationships

- Organizations should define the interrelationship of the audit, compliance, and legal functions in charters or other organizational documents
- Boards should assess the adequacy, independence, and performance of different functions within the organization periodically
- According to OIG an organization's Compliance Officer should neither be counsel for the provider, nor subordinate in function or position to counsel or the legal department

Roles and Relationships

- To efficiently operate, the compliance, legal, and internal audit functions should have access to relevant corporate information and resources
- The Board should establish a process to ensure ease of access to information; this process may be included in a formal charter document approved by the Audit Committee of the Board or in other appropriate documents
- Organizations that fail to separate these functions should recognize and mitigate potential risks by allowing individuals operating in several roles to execute each function independently

Roles and Relationships

- Boards should consider and discuss how management works together to address risks, including the role of each in:
  - Identifying compliance risks
  - Investigating compliance risks and avoiding duplication of effort
  - Identifying and implementing appropriate corrective actions and decision-making
  - Communicating between the various functions throughout the process
- Audit, compliance, and legal functions should all be on one accord with respect to accountability, risk, compliance, auditing, and monitoring

Reporting to the Board

- The Board should receive regular reports concerning the organization's risk mitigation and compliance efforts from the audit, compliance, human resources, legal, quality, and information technology functions
- It is helpful for the Board to establish expectations for the management team and to hold them accountable for informing the Board in accordance with those expectations
- The Board can request scorecards that measures management's efforts in mitigating risks and implementing corrective action plans

Reporting **to** the Board

- Expectations may include:
  - Reporting information on internal and external investigations
  - Serious issues raised in internal and external audits
  - Hotline call activity
  - Allegations on material fraud or senior management misconduct
  - Management expectations to the organization's code of conduct
  - Management expectations to the expense reimbursement policy
- The Board should receive compliance and risk-related information in a format that satisfies the interest of its members and fits their capacity to review that information

Reporting **to** the Board

- Boards should consider a risk-based reporting system, whereas those that are responsible for the compliance function develop reports for the Board when particular risk-based criteria are met
- The Board should establish protocols to ensure that suspected violations are reported in a timely manner, and to evaluate and implement remedial consequences
- Consistent internal reviews that give the Board an overview of where the organization is, and where it is going can enhance compliance results and the quality of services

Identifying & Auditing Potential Risk Areas

- Compliance in health care necessitates monitoring activities that are vulnerable to fraud and other violations
- Areas of interest include:
  - Referral relationships and arrangements
  - Submitting claims for services not rendered/unnecessary services
  - Privacy breaches
  - Quality-related events
  - Up-coding

Identifying & Auditing Potential Risk Areas

- Risk Areas can be identified from internal or external information sources
- Internal sources:
  - Employee reports
  - Internal compliance hotlines
  - Internal audits
- External sources:
  - Professional organization publications
  - OIG-issued guidance
  - News Media

Identifying & Auditing Potential Risk Areas

- The Guidelines require organizations to conduct monitoring and auditing for potential criminal conduct
- Audits can aid in finding potential risk factors, identifying regulatory or compliance problems, and confirming the effectiveness of compliance controls
- Audits that identify compliance issues or controls deficiencies should be paired with corrective action plans
- When structuring risk assessment plans, recent industry trends should be considered

Identifying & Auditing Potential Risk Areas

- Compliance functions assessing new areas of risk should consider the increasing emphasis on quality, industry consolidation, and changes in insurance coverage and reimbursement
- New forms of reimbursement and payment models result in new incentives and compliance risks
- New payment models has incentivized consolidation among health care providers and has resulted in more employment and contractual relationships
- Boards of organizations that have financial relationships with referrals or recipients should investigate how the organization reviews these arrangements

Identifying & Auditing Potential Risk Areas

- Boards of organizations that employ physicians should be cognizant of relationships that exist between their employees and other health care entities
- The Board should assess whether those relationships could impact clinical and research decision-making issues
- Due to the fact that information has become more accessible to the public, boards may be asked important compliance related questions by patients, employees, government officials, donors, the media, and whistleblowers

Encouraging Accountability & Compliance

- The entire organization is responsible for the execution of the compliance program
- To highlight the importance of compliance, organizations may assess individual, departmental, or facility-level consistency in executing the compliance program
- Assessments can be used to award bonuses or withdraw incentives based on compliance and quality results
- OIG is increasingly requiring managers to show compliance certifications outside of the compliance department

Encouraging Accountability & Compliance

- Organizations that discover violations usually engage in an internal assessment of the costs and benefits of disclosing
- Organizations that are proactive at self-disclosing violations may realize benefits such as:
  - Faster resolution of the case
  - Lower payment
  - Exclusion releases a part of the settlement with no CIA or other compliance obligations
- Boards should inquire about how management handles disclosing violations

Encouraging Accountability & Compliance

- The Board should evaluate whether the organization's compliance system and procedures encourage communication throughout the organization, and whether employees are comfortable raising compliance related issues without fear of retaliation or retribution
- Boards should also assess management's response to violations of the organization's policies or federal or state laws that are brought to their attention

Oversight and Enforcement

Oversight and Enforcement Mechanisms

- Surveys (event based and routine)
- Fines (e.g., EMTALA)
- Payment hold
- Corporate Integrity Agreements / System Improvement Agreement
- Exclusion from Federal Healthcare Programs
- Lawsuits filed by the Department of Justice on behalf of HHS or by State Attorney Generals on behalf of their respective Medicaid administrator

Enterprise Risk Management

ASHRM

Enterprise risk management (ERM) in healthcare promotes a comprehensive framework for making risk management decisions which maximize value protection and creation by managing risk and uncertainty and their connections to total value.

www.ashrm.org/system/files?file=media/file/2019/06/ERM-Tool_final.pdf

ERM Risk Domains

- Operational
- Clinical/Patient Safety
- Strategic
- Financial
- Human Capital
- Legal/Regulatory
- Technology
- Hazard

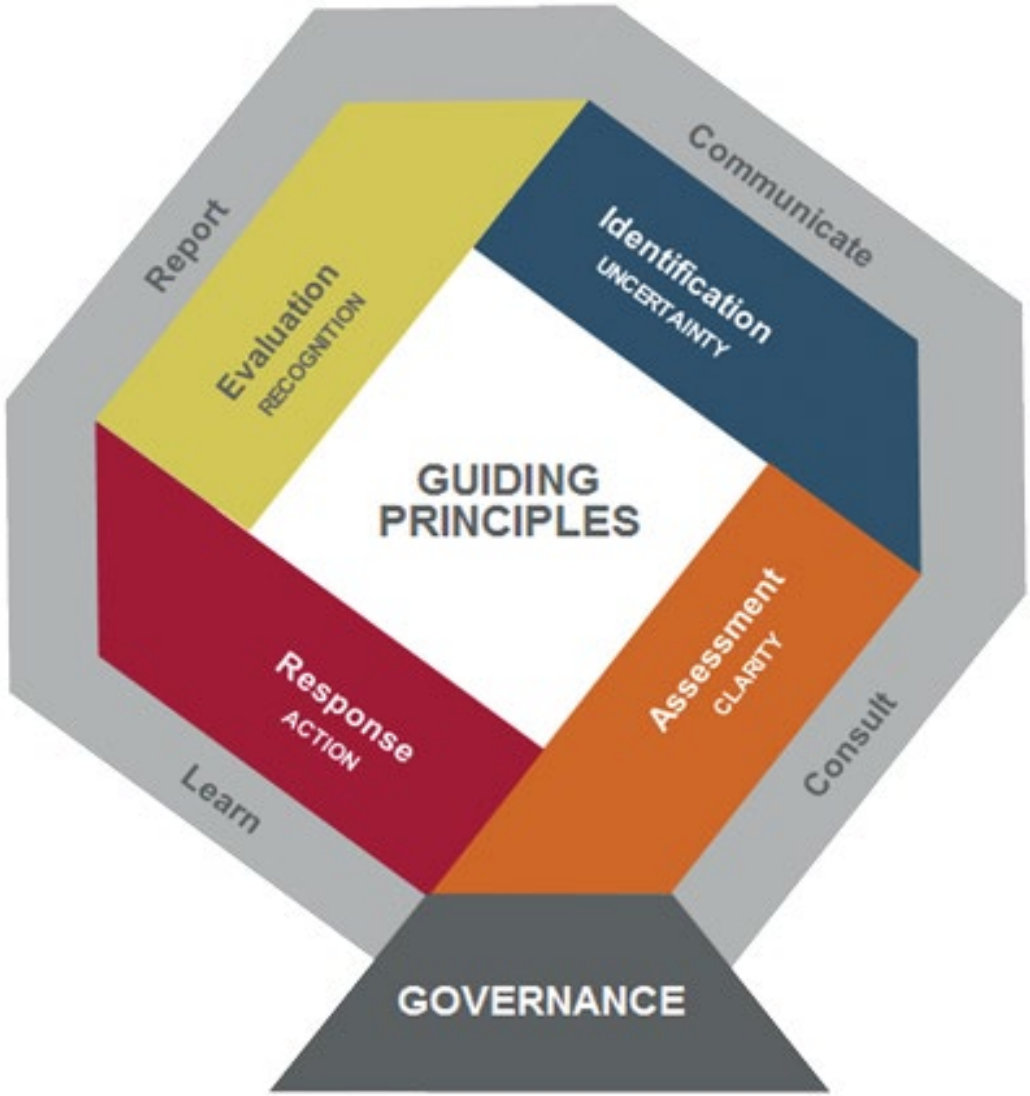
Common Techniques to Manage Risks

- Risk Avoidance: Implementing systems or controls that will completely prevent the risk from occurring
- Risk Prevention: Taking action to reduce the probability that a risk will occur
- Risk Reduction: Reducing the impact of the risk

ERM Guiding Principles

- Advance safe and trusted healthcare
- Manage uncertainty
- Maximize value protection and creation
- Encourage multidisciplinary accountability
- Optimize organizational readiness
- Promote positive organizational culture which will impact readiness and success
- Utilize data/metrics to prioritize risks
- Align risk appetite and strategy

ERM Framework



4 Elements of Enterprise Risk Management

- Identification
- Assessment
- Evaluation
- Response

Identification

- Identify risks using various tools:
  - Questionnaires
  - Focus Groups
  - Interviews
  - Peer review
  - Hotlines/ Reporting channels

- Create a master list of all relevant risk areas and divide into distinct areas

Assessment

- Risk assessment allows for better risk prioritization and mitigation
- Conduct a risk assessment by analyzing both the likelihood and impact of each risk
  - Likelihood: consider existing controls and policies in place
  - Impact: consider legal, financial, operational, reputational, and health/safety effects
  - Velocity (time to impact) may also be used as a dimension

Evaluation

- Modify internal controls to meet elevated risks identified by risk assessment
  - Greater likelihood or frequency might signal the need to strengthen preventative internal controls
  - Increased impact the longer a risk remains undetected likely favors detective internal controls
- Implement or improve relevant auditing or monitoring functions
- Increase compliance related training
- Establish accountability to ensure that risk responses are properly executed

Response

- Crisis Management / Public Relations Strategy
- Billing and Coding Risk Analysis
- Legal/Regulatory
  - Self-Reporting Required?
  - Fraud and Abuse Law Compliance
  - Joint Commission Accreditation / CMS
- Effective Internal Communications
- State and Federal Agency Coordination

Ongoing ERM Practices

- Engage in continuous review of current controls and systems
- Alter risk management programs accordingly as circumstances change
  - New laws, regulations, and guidance
  - New business efforts
  - New third-party partnerships
- Utilize internal and external audits
- Communicate necessary risk information to relevant governance

Scenario #1

- The two EMS workers accused of killing a Springfield, Illinois, man in their care who died last month after they transported him strapped tightly facedown on a stretcher.
- Peter C., 50, and Peggy F., 44, were charged with murder on Jan. 9 in the death of Earl Moore, Jr., 35, on Dec. 18.
- Police had called an ambulance to a home Moore was in where he was in medical distress.
- Moore died of compressional and positional asphyxia "due to prone face-down restraint on a paramedic transportation cot/stretcher by tightened straps across the back."

An image from a police body camera shows paramedics loading Earl Moore into an ambulance on Dec. 18, 2022, in Springfield, Ill. (Sangamon County Government).
https://www.nbcnews.com/news/us-news/2-illinois-ems-workers-charged-murder-death-patient-strapped-stretcher-rcna66715

Response

- Crisis Management / Public Relations Strategy
- Billing and Coding Risk Analysis
- Legal/Regulatory
  - Self-Reporting Required?
  - Fraud and Abuse Law Compliance
  - Joint Commission Accreditation / CMS
- Effective Internal Communications
- State and Federal Agency Coordination

Scenario #2

- Cybercriminals believed to be located in China, exploited a software vulnerability by deploying high-sophisticated malware leading to the theft of sensitive patient data. The incident impacted anyone that received treatment from a facility associated with the Community Health System network in the last 5 years.
- 4.5 million patients impacted

Response

- Crisis Management / Public Relations Strategy
- Billing and Coding Risk Analysis
- Legal/Regulatory
  - Self-Reporting Required?
  - Fraud and Abuse Law Compliance
  - Joint Commission Accreditation / CMS
- Effective Internal Communications
- State and Federal Agency Coordination

Scenario #3

- Born prematurely in 2019, Tinslee's body was unable to properly get oxygen into her bloodstream, and doctors were unable to improve her situation. Cook Children's Medical Center determined continued intervention was causing her to suffer, citing the Texas Advanced Directives Act, which allows hospitals to end care after 10 days unless families can find an alternative location for treatment.
- Texas Right to Life and Protect TX Fragile Kids filed and won a court injunction that has held up through appeals to the Texas and U.S. Supreme Court.

Response

- Crisis Management / Public Relations Strategy
- Billing and Coding Risk Analysis
- Legal/Regulatory
  - Self-Reporting Required?
  - Fraud and Abuse Law Compliance
  - Joint Commission Accreditation / CMS
- Effective Internal Communications
- State and Federal Agency Coordination

Resources

Compliance Resources

- Federal Sentencing Guidelines:
  (https://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2021/GLMFull.pdf)

- OIG Supplemental Compliance Program Guidance for Hospitals:
  (https://oig.hhs.gov/documents/compliance-guidance/797/012705HospSupplementalGuidance.pdf)

- OIG Corporate Integrity Agreements:
  (https://oig.hhs.gov/compliance/corporate-integrity-agreements/)

Compliance Resources

- Affordable Care Act Provider Compliance Program:

  (https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNEdWebGuide/Downloads/MLN-Compliance-Webinar.pdf)

- OIG Healthcare Compliance Program Tips:

  (https://oig.hhs.gov/documents/compliance-guidance/797/012705HospSupplementalGuidance.pdf)

- Practical Guidance for Health Care Governing Boards on Compliance Oversight

  (https://oig.hhs.gov/documents/root/162/Practical-Guidance-for-Health-Care-Boards-on-Compliance-Oversight.pdf)

Kenya Woodruff

Katten Muchin Rosenman LLP
Partner

kenya.woodruff@katten.com