Katten's Sixth Annual Women's In-House Counsel and Compliance Officer Program

Tackling the Tough Issues in Health Care Law and Compliance

Laura Keidan Martin
Katten Muchin Rosenman LLP
Chicago
+1.312.902.5487
laura.martin@kattenlaw.com

Megan Hardiman
Katten Muchin Rosenman LLP
Chicago
+1.312.902.5488
megan.hardiman@kattenlaw.com

Katten
Katten Muchin Rosenman LLP

Agenda

- The Board's Role in Compliance Oversight: What the New OIG Guidance Means for Your Organization
- Hot Topics in HIPAA and Cybersecurity
- Physicians and Vendors: Avoiding Non-Monetary Compensation Pitfalls

Katten
Katten Muchin Rosenman LLP

The Board's Role in Compliance Oversight: What the New OIG Guidance Means for Your Organization

Katten
Katten Muchin Rosenman LLP

Corporate Leadership Responsibility

- An effective compliance program minimizes organizational and personal risks in three important ways:
  - Reduces risk that violations will occur
  - When violations occur, ensures that corrective actions are implemented to appropriately remediate in accordance with law and prevent recurrence
  - Results in more lenient sanctions under a variety of Governmental guidances detailed later in this presentation:
    - Reduced penalties
    - Reduced risk of corporate integrity agreement (“CIA”)

Katten
Katten Muchin Rosenman LLP

Government Guidance on Importance of Effective Compliance Programs

- The following guidance documents issued by various Government agencies inform the Board's compliance oversight role and responsibilities:
  - OIG Compliance Guidance
  - U.S. Federal Sentencing Guidelines
  - U.S. Department of Justice Guidelines
  - Case Law
  - "Practice Guidance for Health Care Governing Boards on Compliance Oversight"
- Case law demonstrates the risks to corporations and their directors of insufficient Board oversight

Katten
Katten Muchin Rosenman LLP

OIG Guidance: Importance of Culture and Leadership

- The U.S. Department of Health and Human Services ("HHS") Office of Inspector General ("OIG") has issued compliance program guidances ("OIG Guidances") for various health care sectors (including hospitals and physician practices) identifying the elements of an effective compliance program.
- All of the OIG Guidances encourage the implementation and use of internal controls to monitor adherence to applicable statutes, regulations and program requirements.
- The OIG website notes that "because of their oversight responsibilities, ***boards of directors have a unique opportunity to promote quality of care and embrace compliance with law***."

Katten
Katten Muchin Rosenman LLP

OIG Guidance: Importance of Culture and Leadership

- The OIG Guidances emphasize the importance of leadership and culture:
  - "Leadership should foster an organizational culture that values, and even rewards, the prevention, detection, and resolution of quality of care and compliance problems."
  - "The organization should endeavor to develop a culture that values compliance from the top down and fosters compliance from the bottom up. Such an organizational culture is the foundation of an effective compliance program."

Katten
Katten Muchin Rosenman LLP

OIG Guidance: Seven Elements of an Effective Compliance Program

- The Guidances reflect the OIG's belief that ***"every effective compliance program must begin with a formal commitment by the governing body"*** to all of the following elements:
  - Written standards of conduct, policies and procedures that promote the health system's commitment to compliance
  - Designation of a compliance officer, compliance committee and other appropriate compliance infrastructure
  - Effective training and education
  - Effective lines of communication
  - Auditing and monitoring
  - Prompt and appropriate response to suspected non-compliance.
  - Enforcement of disciplinary standards through well publicized guidelines

Katten
Katten Muchin Rosenman LLP

Federal Sentencing Guidelines

- Likewise, the Federal Sentencing Guidelines ("FSG") emphasize that companies should:

  Exercise due diligence to prevent and detect criminal conduct; and otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

- The FSG also enumerates seven elements that evidence an effective compliance program, which are nearly identical to (and in fact formed the basis of) the seven elements reflected in OIG Guidances.

Katten
Katten Muchin Rosenman LLP

Department Of Justice Guidelines

- The following factors are considered by the DOJ in Federal prosecutions of corporations:
  - Nature and seriousness of the offense
  - Pervasiveness of the wrongdoing within the entity
  - History of similar conduct
  - Timely and voluntary disclosure of wrongdoing and willingness to cooperate with the government's investigation
  - ***Existence and adequacy of the corporation's compliance program***
  - Remedial actions taken by the corporation
  - Collateral consequences of a conviction
  - Adequacy of the prosecution of the individuals responsible
  - Adequacy of non-criminal alternatives

Katten
Katten Muchin Rosenman LLP

Practical Guidance for Health Care Governing Boards on Compliance Oversight

This April, the OIG partnered with AHLA, the Association of Healthcare Internal Auditors and the Health Care Compliance Association to issue guidance covering the following areas:

- Roles and relationships between the organization's audit, compliance and legal departments.
- Mechanisms and processes for issue reporting within the organization
- Approach to identifying regulatory risk
- Methods of encouraging enterprise-wide accountability for achievement of compliance goals and objectives

The Bottom Line: Boards must exercise their oversight responsibility in good faith, including making inquiries to ensure that a corporate information/ reporting system exists to assure that the Board receives appropriate information relating to compliance matters.

Katten
Katten Muchin Rosenman LLP

Practical Guidance: Roles and Relationships

- Boards should develop a formal plan to stay abreast of the ever-changing regulatory landscape and operating environment.
- The interrelationship of the audit, compliance and legal functions should be defined in charters or other organizational documents.
- Boards should evaluate and discuss how management of each function works together to address risk, including their roles in:
  - Identifying compliance risks
  - Investigating compliance risks and avoiding duplication of effort
  - Identifying and implementing appropriate corrective actions and decision-making, and
  - Communicating between the various functions throughout the process

Katten
Katten Muchin Rosenman LLP

Practical Guidance: Board Reporting

- The Board should receive regular reports regarding the organization's risk mitigation and compliance efforts – separately and independently – from a variety of key players, including those responsible for audit, compliance, human resources, legal, quality and information technology.
  - The Board may request the development of objective scorecards that measure how well management is executing the compliance program, mitigating risks and implementing corrective action plans.
  - Expectations could also include reporting information on internal and external audits, hotline call activity, all allegations of material fraud or senior management misconduct and all management exceptions to the organization's code of conduct and/or expense reimbursement policy.
  - In addition, the Board should expect that management will address significant regulatory changes and enforcement events relevant to the organization's business.

Katten
Katten Muchin Rosenman LLP

Potential Elements of a Board Dashboard Report

- Statistics regarding completion of compliance education requirements/personnel compliance with deadlines
- Number/type/source of reports of suspected non-compliance
- Number/type/status/disposition of compliance investigations and time pending
- Status of corrective action plans/deadline compliance
- Number/type/results of compliance audits
- Status of policy updates and approvals
- Status of major HCC projects/initiatives
- Licensure/accreditation survey schedule and results

However, the dashboard is not a substitute for granular information about major investigations, deviations from legal parameters, fraudulent acts or senior management misconduct.

Katten
Katten Muchin Rosenman LLP

Practical Guidance: Board Reporting

- It is important for Board members to understand the dynamic regulatory environment so that they can ask pertinent questions of management and make informed strategic decisions regarding the compliance program, including funding and resource allocations.
- A Board can raise its level of substantive expertise on regulatory/compliance matters by adding to the Board, or periodically consulting with, an experienced regulatory, compliance or legal professional.
- The Board should consider regular “executive sessions” (excluding senior management) with compliance, legal, internal audit and quality leaders to encourage more open communication.

Katten
Katten Muchin Rosenman LLP

Practical Guidance: Identifying Regulatory Risk

- The Board should ensure that management and the Board have strong processes for identifying risk areas for auditing and monitoring.
- The Board should ensure that risk areas are in fact reviewed and monitored.
- When audits or investigations identify issues, the Board should ensure that management develops, implements and monitors corrective action plans.
- Risk assessment plans are encouraged based on:
  - Audit results
  - Industry trends
  - Guidance from external sources
  - Compliance failures of similar organizations

Katten
Katten Muchin Rosenman LLP

Practical Guidance: Encouraging Accountability and Compliance

- Compliance is an enterprise-wide responsibility.
- To ensure that compliance is “a way of life,” a Board may require that:
  - Compliance metrics are included in performance reviews at the individual, department and/or facility levels
  - Compliance is taken into account in incentive and bonus structures
- Boards should ensure that the compliance program encourages self-identification of compliance problems and self-disclosures.
- The Board should request and receive sufficient information to evaluate the appropriateness of management’s responses to identified violations of organizational policies and applicable law.

Katten
Katten Muchin Rosenman LLP

Key Take-Aways

- The Board has a fiduciary duty to ensure an effective compliance program—failure to exercise this duty can result in liability for the Board and the organization.
- The Government expects the Board to exercise increasingly robust oversight of the compliance function.
- In order to exercise such oversight, it is essential for the Board to receive meaningful Compliance reports and to ask the right questions of Compliance and Executives to hold them accountable.
- Boards should be educated on their role in ensuring an effective compliance function, the evolving expectations of the Government in this area and the inquiries they should make to minimize organizational risk.

Katten
Katten Muchin Rosenman LLP

Hot Topics in HIPAA and Cybersecurity

Katten
Katten Muchin Rosenman LLP

Year of the Cyber Attack, Including

- Anthem: 80 million individuals – names, addresses, DOB, health IDs/SSNs, etc. Discovered January 29, 2015. Began December, 2014
- Premera: 11 million individuals – names, DOB, SSN, bank account info. Discovered January 29, 2015. Occurred as early as March, 2014
- CareFirst: 1.1 million individuals – member-created CareFirst user names, names, DOB, email addresses and subscriber ID. Reportedly no sensitive medical or financial information (separate database). Announced May 2015. Occurred as early as June, 2014
- And that's just health care…

Katten
Katten Muchin Rosenman LLP

Important Trend

- Cybercriminals are increasingly focused on health care:
  - For the first time, criminal attacks are the number one cause of data breaches in health care.
  - The percentage of criminal-based security incidents is even higher.
    - Web-borne malware attacks caused security incidents for 78 percent of healthcare organizations and 82 percent for BAs.

Source: Ponemon Institute 5th Annual Benchmark Study on Privacy & Security of Healthcare Data (May 2015)

Katten
Katten Muchin Rosenman LLP

Why Health Care?

- High value
- “Soft Target”

Katten
Katten Muchin Rosenman LLP

Reality Check

- The odds favor the hacker
  - Continual attacks, continually evolving threats
  - Sophisticated attackers, some with deep resources
  - It only takes one chink in the armor

Katten
Katten Muchin Rosenman LLP

Continue to Prevent/Protect

- This includes:
  - Security risk analysis – foundation of risk management program
    - *Required* by HIPAA (45 CFR 164.308)(a)(1)
    - Drives specific measures adopted in required risk management program (45 C.F.R. 164.308(B)).
    - Thorough, up-to-date, cover all locations/media
    - Continually evaluate for changes in threat environment and operational/technological changes
  - Encryption and remote wiping for portable electronic devices
  - Data leak protection
  - Disposal of PHI per OCR guidance
  - Training and policies
  - Manage third party risk – BAA and vendor management program

Katten
Katten Muchin Rosenman LLP

And Especially Important Now…

- Improve your detection capabilities
- Strengthen your incident response plan
  - Are you realistically equipped to deal with complexities of large-scale breach?
- Understand your cyber-liability insurance
  - What is/is not covered?
  - What exclusions and limitations apply?
  - Who is point of contact?

Katten
Katten Muchin Rosenman LLP

Other Key Developments

- OCR Phase II Audits
  - Screening surveys sent
  - OCR will select about 350 CEs
    - Security, privacy and breach notice
  - Combination of desk audits and comprehensive, on-site audits
  - Watch for Phase 2 audit protocol

Katten
Katten Muchin Rosenman LLP

IL Personal Information Protection Act

- **Breach** = unauthorized acquisition of **computerized data** that compromises the security, confidentiality or integrity of **personal information**
- **Personal information** = first name or first initial and last name PLUS any one or more of the following if not encrypted or redacted: SSN, DLN/state ID number, account number or credit/debit number, or account number or credit cared number in combination with any required access code
- Breach triggers notice to individuals (and data owner)

Katten
Katten Muchin Rosenman LLP

SB 1833 – Key Changes

- Expands the definition of “personal information” to include:
  - Medical information
  - Health insurance information (subscriber ID, policy number, claims history, etc.)
  - Unique biometric data
  - Geolocation info*
  - Consumer marketing information*
  - Home address, telephone number, and email address in combination with either:
    - Mother’s maiden name when not part of an individual’s surname; or
    - Month, day and year of birth
  - User name or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted (or are, but the keys were obtained)
  - Personal info which is encrypted/redacted, but the keys have been acquired

Katten
Katten Muchin Rosenman LLP

SB 1833 – Key Changes

- Requires detailed notice to AG of:
  - Single breach impacting more than 250 IL residents
  - Generally, must notify AG within earlier of 30 business days of discovery or concurrent with other notices provided
- Publication by AG of breaches
- Requires use of reasonable security measures by data collectors who collect personal information of IL residents

Katten
Katten Muchin Rosenman LLP

SB 1833 – Key Changes

- Data collectors must contractually require subs to have reasonable security measures
- Privacy policy
  - Operator of commercial web site or online service that collects personal information through the internet about individual consumers residing in IL must conspicuously post its privacy policy
    - Mandates minimum content of privacy policy
    - Defines what it means to “conspicuously post”

Katten
Katten Muchin Rosenman LLP

CE/BA "Deemed Compliance"

- CE/BA subject to and in compliance with HIPAA privacy and security standards "shall be deemed to be in compliance with the provisions of this Act," provided that any CE or BA required to provide notice of a breach to HHS also provides such notice to the AG within 5 business days of notifying the Secretary.

Katten
Katten Muchin Rosenman LLP

Physicians and Vendors: Avoiding Non-Monetary Compensation Pitfalls

Katten
Katten Muchin Rosenman LLP

Key Regulatory Parameters: Anti-Kickback Statute (AKS)

- Prohibits an individual from "knowingly and willfully" *offering*, *paying*, *soliciting*, or *receiving* any remuneration (direct or indirect, in cash or in kind) in return for or to induce referrals or recommendations for services or items covered by a federal health care program — **In short, no payment for business**.
- If ***one purpose*** of the remuneration is to induce business, the arrangement is subject to AKS attack, unless a safe harbor applies.
- As with the Stark Act, numerous exceptions and safe harbors may apply, but unlike Stark, penalties for violations can be both civil *and criminal.*

Katten
Katten Muchin Rosenman LLP

Key Regulatory Parameters: Stark Act

- The Stark Act provides that a physician may not
  1) Refer Medicare or Medicaid patients to an entity
  2) For the furnishing of "designated health services" (DHS)
  3) If there is a financial relationship between the referring physician (or an immediate family member) and the entity
  4) Unless an exception applies
- **Bottom line:** Every direct and indirect compensation arrangement between a hospital (or other DHS entity) and a physician ***must*** be structured to satisfy a Stark exception, or else the physician cannot refer Medicare/Medicaid patients to the hospital (or other entity).

Katten
Katten Muchin Rosenman LLP

Key Regulatory Parameters: False Claims Act

- FCA prohibits a person from knowingly
  - Presenting a false or fraudulent claim to the government for payment or approval, or
  - Making or using a false record or statement material to a false or fraudulent claim, or
  - Retaining overpayments
- Imposes civil penalty per violation *plus* treble damages.
- Empowers whistleblowers to bring "*qui tam*" suits on behalf of the government and pocket a share of the proceeds.
- Government and *qui tam* plaintiffs use Stark Act and AKS violations as basis for asserting FCA claims.

Katten
Katten Muchin Rosenman LLP

Non-Monetary Compensation: Parameters and Pitfalls

Stark Exception	Regulatory Parameters	Regulatory Pitfalls
Non-Monetary Compensation	▪ Applies to annual non-monetary compensation in the form of items or services (not including cash or cash equivalents) that does not exceed an aggregate of $300 per year, if all of the following conditions are satisfied: • The compensation is not determined in any manner that takes into account volume or value of referrals or other business generated by the physician. • The physician or the physician's group (including staff) cannot solicit the non-monetary compensation. • The arrangement cannot violate the AKS or any Federal or State law or regulation governing billing or claims submission. ▪ The annual dollar cap is adjusted each calendar year based on the increase in the Consumer Price Index-Urban All Items. • The current cap is $392. ▪ One medical staff appreciation event per year is exempt from the cap. ▪ When an entity inadvertently exceeds the cap by no more than 50% and the physician returns the excess (item(s) or value) by the end of the calendar year in which the benefit was provided or within 180 days (whichever is earlier), then the entity will not be deemed to exceed the cap. • This exception can only be used once every three years per physician.	▪ Failure to track non-monetary compensation. ▪ Failure to "count" invitations to parties, civic/ charitable events and other speaker programs and dinners paid for by the hospital. ▪ Provision of logoed items like duffel bags, fancy pens or sweaters. ▪ Free rounds of golf. ▪ Provision of free staff. ▪ Provision of free CME. ▪ Providing unrestricted gift cards and gift certificates. ▪ Honoring a physician group's request for holiday party funding or equipment.

Katten
Katten Muchin Rosenman LLP

Key Decision Points for Policy on Non-Monetary Compensation

- Policy scope
- Exceptions
- Approach to physician participation in boards, committees, leadership, recruitment and other initiatives that benefit Health System
  - Should policy incorporate a template letter agreement for such services to avoid need to track non-monetary compensation provided as part of the arrangement? [Note: there is a good argument that the personal services arrangement exception should apply in this situation but it is unclear whether CMS would agree.]
- Tracking mechanisms/internal controls
- Pre-approval requirements
  - Should it be required?
  - Who should approve?
  - Should approval criteria be defined?
  - Timeframes and templates

Katten
Katten Muchin Rosenman LLP

Key Decision Points for Policy on Non-Monetary Compensation

- Limits on particular types of non-monetary compensation
  - Gifts
  - Gift cards
  - CME
  - Staffing and other free services
  - Entertainment and sporting events*
  - Meals
  - Charity events and donations
  - Offsite CME/educational programs
- Allocation issues (*e.g.*, gifts to physician office staff)
- Provisions for repayment of non-monetary compensation in excess of cap
- Should the Policy apply to non-DHS entities within the Health System?

*NOTE: PhRMA and AdvaMed Codes ban all forms of entertainment.

Katten
Katten Muchin Rosenman LLP

Decision Points: Potential Exceptions

- Non-monetary compensation provided pursuant to a *bona fide* employment arrangement or personal services agreement
- Medical staff incidental benefits
- Compliance training
- Information technology provided pursuant to a Stark exception
- Non-monetary compensation pursuant to other Stark Act exceptions, perhaps subject to legal department or compliance officer approval
- Gifts, meals and entertainment provided by a Hospital representative to a physician with whom he/she has a personal relationship that is not expensed to any Health System entity or claimed as a business expense

Katten
Katten Muchin Rosenman LLP

Pitfalls in Vendor Relations

- Although the Stark Law does not apply to arrangements with non-physicians, the AKS governs arrangements with vendors and manufacturers.
  - Remuneration offered or paid to induce or reward the purchase, lease, order or recommendation of an item payable under a FHCP implicates the AKS, even if the item/service is just one component of a service billed by a health care provider and is supplied by a third party.
  - Thus, remuneration provided by vendors/manufacturers to induce or reward a health system's use of vendor/manufacturer products or services is subject to AKS (and FCA) attack.
- Although there are legitimate reasons for the following types of arrangements, they must be carefully structured to avoid AKS pitfalls:
  - Educational/research grants
  - Charitable contributions
  - Agreements for services and/or data
  - Gifts, meals and entertainment
  - Discount and incentive arrangements
  - "Value adds" (free items/ services ancillary to purchased items/ services)

Katten
Katten Muchin Rosenman LLP

Vendor Practices that Raise Red Flags

- Conversion services and conversion fees to promote higher priced drugs or devices.
- Conducting “market research” with key physicians, health system executives or supply chain management, particularly in luxury settings and/or when main purpose is promotion.
- Funding chairs, CME/educational programs, major capital projects, research projects or authorship opportunities for key physicians.
- Funding major capital projects or endowments for tax-exempt institutional customers.
- Value-added or below-cost programs and services for institutional customers.
- Sham, unnecessary or overly rich consultant agreements and data collection arrangements.
- Free use of capital equipment in connection with the purchase of consumable items.

Katten
Katten Muchin Rosenman LLP

Common Features of Vendor Relations Policies

- No meals/food, even at on-campus business meeting or educational session
- Regulation of samples and demonstration items, requiring approval by a centralized committee and centralized distribution (not to a single physician or clinical division)
- Regulation of physician relationships with industry
  - Some require approval of all physician relationships with industry
  - Others require relationships to meet certain guidelines *(e.g.,* written agreement, FMV comp set in advance, no use of institution's name)
  - Others bar or discourage certain types of relationships, such as speaker bureaus and advisory boards
  - Many ban ghost writing and participation in marketing/ promotional activities
- Physicians with Industry relationships banned from product selection and P&T committees
- Written "gift" agreements required, even for scholarships, fellowships and grants
- No travel expense reimbursement to evaluate new products/meet with company reps
- Access limitations and registration requirements
- Legal review of pricing arrangements outside of pre-approved parameters

Katten
Katten Muchin Rosenman LLP

Katten Muchin Rosenman LLP Locations

AUSTIN
One Congress Plaza
111 Congress Avenue
Suite 1000
Austin, TX 78701-4073
+1.512.691.4000 tel
+1.512.691.4001 fax

CHARLOTTE
550 South Tryon Street
Suite 2900
Charlotte, NC 28202-4213
+1.704.444.2000 tel
+1.704.444.2050 fax

CHICAGO
525 West Monroe Street
Chicago, IL 60661-3693
+1.312.902.5200 tel
+1.312.902.1061 fax

HOUSTON
1301 McKinney Street
Suite 3000
Houston, TX 77010-3033
+1.713.270.3400 tel
+1.713.270.3401 fax

IRVING
545 East John Carpenter Freeway
Suite 300
Irving, TX 75062-3964
+1.972.587.4100 tel
+1.972.587.4109 fax

LONDON
125 Old Broad Street
London EC2N 1AR United Kingdom
+44.0.20.7776.7620 tel
+44.0.20.7776.7621 fax

LOS ANGELES – CENTURY CITY
2029 Century Park East
Suite 2600
Los Angeles, CA 90067-3012
+1.310.788.4400 tel
+1.310.788.4471 fax

LOS ANGELES – DOWNTOWN
515 South Flower Street
Suite 1000
Los Angeles, CA 90071-2212
+1.213.443.9000 tel
+1.213.443.9001 fax

NEW YORK
575 Madison Avenue
New York, NY 10022-2585
+1.212.940.8800 tel
+1.212.940.8776 fax

ORANGE COUNTY
100 Spectrum Center Drive
Suite 1050
Irvine, CA 92618-4960
+1.714.966.6819 tel
+1.714.966.6821 fax

SAN FRANCISCO BAY AREA
1999 Harrison Street
Suite 700
Oakland, CA 94612-4704
+1.415.293.5800 tel
+1.415.293.5801 fax

SHANGHAI
Suite 4906 Wheelock Square
1717 Nanjing Road West
Shanghai 200040 P.R. China
+86.21.6039.3222 tel
+86.21.6039.3223 fax

WASHINGTON, DC
2900 K Street NW
North Tower - Suite 200
Washington, DC 20007-5118
+1.202.625.3500 tel
+1.202.298.7570 fax

Katten
Katten Muchin Rosenman LLP
www.kattenlaw.com