Key Compliance Risks for Healthcare Organizations

Montana Hospital Association
Compliance & Risk Management Conference

October 29, 2020

Presented by:
Shannon Sumner, CPA, CHC®
Susan Thomas, CHC®, CIA, CRMA, CPC®, CCSFP, CHIAP
Traci Waugh, CHC®, RHIA, CHPS

Agenda

- Introductions
- Compliance Involvement In Organizational Strategy
- Compliance Risk Assessment
- Risk-Based Compliance Work Plan
- Important Healthcare Industry Risks

Speaker Introduction

Shannon Sumner
(800) 270-9629
ssumner@pyapc.com

PYA, P.C.
215 Centerview Drive
Brentwood, TN 37027

Shannon manages PYA's Compliance Advisory Services and serves as the Firm's Compliance Officer.

A CPA certified in healthcare compliance, she has more than two decades' experience in healthcare internal auditing and compliance programs. She advises large health systems and legal counsel in strengthening their compliance programs, and aids in areas of Anti-Kickback Statute and Stark Law compliance. Shannon also assists health systems regarding compliance with Corporate Integrity Agreements (CIAs) and Non-Prosecution Agreements (NPAs), conducts health system merger/acquisition/divestiture due diligence activities, and advises health system governing boards on their roles and responsibilities for effective compliance oversight.

At the direction of the Department of Justice, Shannon has served as the healthcare compliance and internal audit subject-matter expert for the largest federal compliance co-monitorship of a health system in U.S. history.

Speaker Introduction

Susan Thomas
(800) 270-9629
sthomas@pyapc.com

PYA, P.C.
9900 West 109th Street, Suite 130
Overland Park, Kansas 66210

Susan has spent nearly three decades working in a variety of managerial and clinical capacities including compliance management, clinical department leadership, provider practice administration, internal audit, quality outcomes, and healthcare advocacy.

A former corporate compliance officer and clinical department director, she has a demonstrated record of success in program development and expansion as well as the ability to form mutually beneficial relationships.

Susan is a hands-on manager and decisive team leader with highly developed negotiation skills and experience cultivating strategic healthcare business partnerships, recruiting and directing teams, developing performance improvement measures, and creating effective training programs.

Speaker Introduction

Traci Waugh
(406) 751-6646
twaugh@krmc.org

Kalispell Regional Healthcare
310 Sunnyview Lane
Kalispell, MT 59901

Traci has been immersed in the healthcare industry with an assortment of responsibilities. She started her career as the director of medical records and eagerly took on additional roles including utilization review, risk management, medical staff services, discharge planning, quality improvement, contracting, privacy, and compliance. Traci's enthusiasm as not subsided; she is always willing to help her peers and serve as a resource.

Along with her initial certification as Registered Health Information Administrator (RHIA), she obtained her Certification in Healthcare Privacy and Security (CHPS) and Certification in Healthcare Compliance (CHC).

Currently as the Director of Outreach Services and Compliance, Traci assists partner critical access hospitals with their compliance programs and provides customized compliance education to staff and board or directors. In addition, she serves as a liaison for other contracted services provided by Kalispell Regional Healthcare.

Clients in ALL 50 STATES

Consistently ranked TOP 20 HEALTHCARE CONSULTING firm in the U.S. by Modern Healthcare

INSIDE PUBLIC ACCOUNTING TOP 100 FIRMS 2019

OVER 1200 Healthcare valuation opinions rendered annually

TOP 15 LARGEST AUDITOR of AHA's Top U.S. Multi-Hospital Systems - Ames Research Group

4,932

Number of healthcare projects during 2018

354 TOTAL BEDS

KRMC: 192

KRMC Adult Acute Care: 122

Pathways Treatment Center: 40

Montana Children's: 30

Brendan House: 110

The HealthCenter: 27

North Valley Hospital: 25

CORE SERVICES

Cancer Care

Cardiovascular and Pulmonary Care

Neuroscience and Spine Care

Orthopedics

Surgical Care

Pediatric Specialty Care

Behavioral Health

197 EMPLOYED PHYSICIANS

117 ADVANCED PRACTICE PROVIDERS

879 EMPLOYEES

47 CLINICS

≈66 SPECIALTIES

≈500 MEDICAL STAFF MEMBERS

ADMITS ≈12,000 PEOPLE ANNUALLY

SEES ≈33,000 ER PATIENTS ANNUALLY

PERFORMS ≈18,000 SURGERIES ANNUALLY

DELIVERS ≈1,200 BABIES ANNUALLY

≈4,000 EMPLOYEES

SERVES ≈600K POPULATION

SERVES ≈40K SQUARE MILES

SERVES 13 COUNTIES

LEADS MONTANA IN PATIENT CARE

– U.S. News and World Report

1007ELT020420

Compliance Involvement in Organizational Strategy

Why Does It Matter?

- Strategic planning is the method that determines what things need to be done. It provides the goals and objectives of business.
- Strategic goals and objectives need to align with regulations, accreditation standards, business initiatives, and other requirements.
- Compliance Leadership present during strategic planning helps to mitigate risks to the organization -- including potential rework, waste, errors, reputation, and financial loss.
- Establishing an alliance between corporate strategy and compliance ensures sustainable results.

The Role of Compliance In Strategy

- Define or redefine the scope of compliance across the organization.
- Become a strategic partner with functional leads in areas directly affected by compliance to ensure that all issues are being managed effectively.
- Expand the compliance focus to include both current and emerging risks.
- Collaborate and coordinate risk assessment activities to prevent assessment fatigue.

Compliance Risk Assessment

Why Is Risk Important?

- Compliance professionals can help inform the strategic perspective by looking at risk.
- It's not just about what is legal – it's also the risk environment and appetite of the organization.
- Its not about saying ***NO***, it's about helping to enable ***HOW***.
- Management is being told to be innovative and think outside the box, but often regulatory requirements get in the way.

Risk Assessment Process

- A risk assessment should not be solely focused on downside risk, but also increase awareness of possible opportunities, which could in turn affect the strategic plan.
- The risk assessment process is cyclical – risks must be identified and analyzed before preparing mitigation plans.
- Understand the roles involved – it's not just Compliance, but also . . .
  - Management and key staff
  - Physician leaders
  - Board and Board Committee

Conducting a Risk Assessment

The 7 Elements

- Oversight
- Policies & Procedures
- Training & Education
- Auditing & Monitoring
- Consistent Enforcement
- Response to Deficiencies
- Open Communication

Regulatory Focus

- OIG Work Plan
- RAC, ZPICS, denials
- NCDs, LCDs
- CIAs, fraud alerts

Previously Identified Issues

- Problematic areas
- Management concerns

"Hot Topics"

- In the news
- Other notable investigations

Risk-Based Compliance Work Plan

Compliance Work Plan

- The compliance work plan should be an annualized “to-do” list for the compliance program based on the compliance risk assessment.
- It is a list of planned projects or actions that are conducted in response to identified risk areas.
- Potential activities include:
  - Conducting trainings on a particular risk area
  - Reviewing and, if necessary, revising policies and procedures
  - Conducting audits to determine compliance
  - Implementing monitoring activities

Compliance Work Plan

Key Recommendations

- Be flexible and realistic.
- Involve key stakeholders.
  - Assign due dates and responsible parties.
  - Communicate throughout the process.
- Monitor and report on work plan status to leadership and the Board.
- Re-evaluate and reprioritize work plan items as needed.
- Build in room for the unknown.

Important Healthcare Industry Risks

Audience Question

What issues are risks for your organization?

So Many Risks, So Little Time…

- Physician financial arrangements
- Contract management
- Advanced technologies
- Vendor management
- Telemedicine
- Interoperability/Information Blocking
- Compliance program due diligence
  - Training
  - Exclusion checks
  - Conflict of interest
- HIPAA privacy and security
  - Patient access
  - Information sharing
  - Cyberattacks
  - Remote workers
- Back end revenue cycle operations
- Emergency preparedness

Physician Financial Arrangements

- **Risks**
  - Stark Law violations
    - Referrals for DHS
  - AKS
    - Pay, offer, solicit, or receive remuneration
  - Shift of responsibility
    - From hospital to physician
  - Stacked Arrangements
    - Multiple types of contracts for one individual

- **Controls**
  - FMV and commercial reasonableness
  - No tie to current or expected referrals
  - Legal counsel review
  - Duties and responsibilities defined
  - Oversight
    - Compensation Committee
  - Monitoring and auditing

Advanced Technologies

- **Risks**
  - Increased transmission of medical data across multiple platforms, medical devices, wearables, applications exposes risk to exposure of data
  - Increased bandwidth (5G) resulting in transmission of more data than ever before
  - Opportunities for hackers to gain access to patient data and access to medical devices
  - Compliance, financial, patient care and reputational risks
  - Third party vendor risks

- **Controls**
  - Inventory of all medical device technologies especially those that transmit and receive data
  - Assess adequacy of budget dollars available for protection of PHI as well as the prevent hackers from taking over medical devices
  - Proactive auditing and monitoring critical as these technologies are more sophisticated than ever before
  - Are there comprehensive agreements in place between the organization and these third-party providers regarding accessing and distributing patient data?

Contract Management

- **Risks**
  - Non-compliance with contract terms
  - Unintentional auto-renewals due to missed cancellation notices or deadlines
  - Missed contract obligations
  - Inefficient workflow processes
  - Failure of an audit due to missing key elements of an audit trail
  - Version control problems
  - Physician Owned Entities

- **Controls**
  - A central electronic repository to manage required documentation
  - Standardized and automated processes for contract execution, review, approval, and renewal
  - Monitoring and auditing of contracts to ensure that regulatory and policy requirements are met prior to payment of or receipt of remuneration
  - Adequate oversight of outsourced services

Vendor Management

- **Risks**
  - Conflicts of interest
  - Excluded vendors
  - Contractual non-compliance
  - Management of vendors as Business Associates

- **Controls**
  - Ethical standards and rules of engagement for all vendors
  - Assure that no vendors are excluded entities
  - Robust procurement process
    - Accountability
    - Contract language standardization
    - Invoice controls
    - Monitoring and auditing of high-risk vendor relationships
    - Contract termination process
  - Create a third party or vendor management checklist:
    - Reference checks
    - Financial solvency
    - Liability coverage
    - Regulatory compliance
    - Verification of delivery, service, and expertise

Telemedicine

- **Risks**
  - Variance with state regulatory requirements for licensure and credentialing
  - Expertise with documentation and coding requirements
  - IT infrastructure limitations
  - Privacy and security threats
  - Policies and procedures

- **Controls**
  - Up-to-date knowledge of state and federal licensing requirements and telemedicine coding and billing rules
  - Proper vetting of telemedicine platforms
  - Robust cyber hygiene practices to protect sensitive data
  - Adequate cybersecurity insurance

Interoperability/Information Blocking

- **Risks**
  - Deadline for compliance 11/2/2020
  - Civil Monetary Penalties for non-compliance
  - IT system configurations
  - No exception for interference with access or exchange
  - Limited timeline to respond to requests

- **Controls**
  - Establish an Information Blocking Committee
  - Review and update policies
  - Conduct analysis of IT system architecture
  - Expand HIPAA education, especially clinical documentation regarding risk of harm and awareness of obligation
  - Implement procedures for timely processing

Compliance Program Due Diligence

- **Risks**
  - Compliance training for the workforce, including employees, medical staff, volunteers, students and vendors
  - Exclusion from Medicare and Medicaid
  - Conflict of interest, financial relationship disclosure process and Open Payments verification
  - Risk assessment and compliance work plan
  - Staff competency and credibility

- **Controls**
  - Onboarding and annual training is provided, monitored, and kept up-to-date
  - Exclusion checks are done prior to hiring or contracting and monthly thereafter
  - Conflict of interest statements are obtained initially and annually
  - A risk assessment is conducted at least annually resulting the compliance work plan
  - Compliance staff are competent to carry out duties and are provided regular educational opportunities

Cybersecurity

- **Risks**
  - Budget and resource limitations
  - Legacy equipment in use
  - Crime as a business – high value, ease of compromise
  - Ransomware
  - Lack of an adequate cybersecurity response team
  - Inadequate cybersecurity insurance coverage
  - Staff concerns (i.e., patch management, work-arounds)
  - Employees are the weakest link

- **Controls**
  - Investment in qualified information
  - Security personnel with robust leadership
  - Use of current, fully-supported, secure operating systems
  - Secure design and implementation of connectivity solutions
  - Identify and address potential vulnerabilities that can impact patient care and organizational operations
  - Educate, educate, educate

Back-End Revenue Cycle Operations

- **Risks**
  - Claims do not meet payer requirements
  - Untimely billing, resulting in delayed cash flow and lost revenue
  - Untimely or inaccurate posting
  - Untimely follow up on denials or underpayments
  - Noncompliance with Medicare credit balance reporting requirements

- **Controls**
  - Billing Edits and analysis of failed edits and edit overrides
  - Monitor and follow up on aged unbilled accounts
  - Monitor posting of 835s and remittances and resolve CARCs
  - Document payer specific follow up protocols
  - Utilize a payer contract management tool to calculate expected payment
  - Solid process for researching and reporting to Medicare.

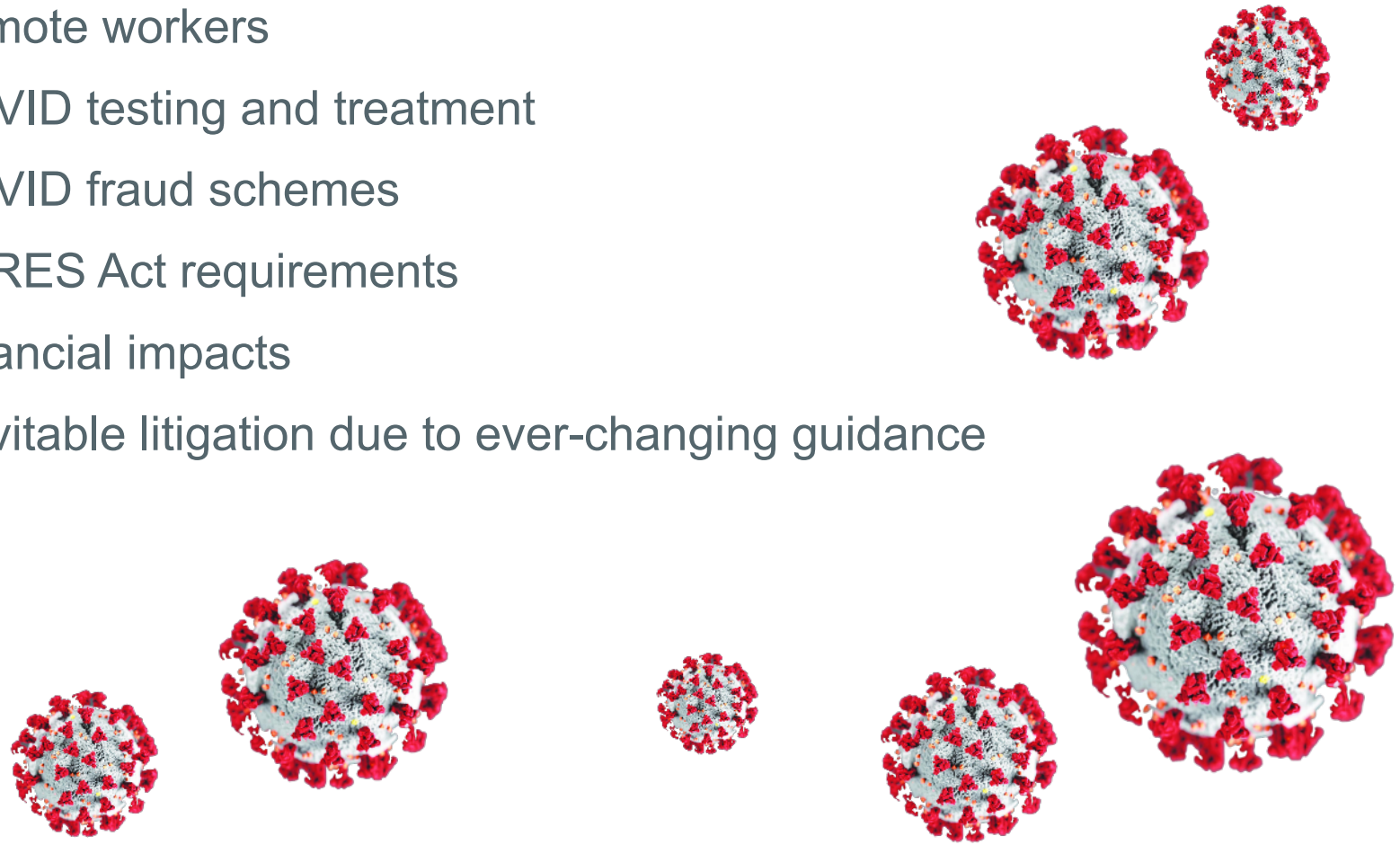
Emergency Preparedness

- **Risks**
  - Not meeting CMS' Conditions of Participation
  - Natural or human-caused
  - Patient safety
  - Reputational risks
  - Information systems failure or compromise (ransomware)

- **Controls**
  - Emergency plan based upon risk assessment (September 2016 CMS requirement) to include policies, procedures, communication plan in coordination with state and local health departments, training
  - Testing (tabletop exercises) conducted at least annually
  - Debrief following real or tabletop exercise
  - Document learnings from COVID-19

And Then There's COVID-19…

- Staff health and safety
- Telemedicine
- Remote workers
- COVID testing and treatment
- COVID fraud schemes
- CARES Act requirements
- Financial impacts
- Inevitable litigation due to ever-changing guidance



Questions?

Thank you!

Shannon Sumner

CPA, CHC®

Principal, Healthcare Consulting

PYA

ssumner@pyapc.com

Susan Thomas

CHC®, CIA, CRMA, CPC®, CCSFP

Manager, Healthcare Consulting

PYA

sthomas@pyapc.com

Traci Waugh

CHC®, RHIA, CHPS

Director of Outreach Services and Compliance

Kalispell Regional Healthcare

twaugh@krmc.org