Session 109: Healthcare Compliance Auditing for Zones of Risk

Presented By:
Debi Weatherford, Executive Director Internal Audit
Piedmont Healthcare
Debra Muscio, SVP, Chief Audit, ERM, Privacy, Security, Ethics & Compliance Officer
Community Medical Centers

Agenda

• About our organizations

• Healthcare compliance zones of risk

• Comments and questions
Who We Are

Healthcare marked by compassion and sustainable excellence in a progressive environment, guided by physicians, delivered by exceptional professionals, and inspired by the communities we serve.

Piedmont is a not-for-profit, community health system comprised of the following entities:

- Piedmont Athens Regional
- Piedmont Atlanta Hospital
- Piedmont Columbus Regional
- Piedmont Fayette Hospital
- Piedmont Henry Hospital
- Piedmont Mountainside Hospital
- Piedmont Newnan Hospital
- Piedmont Rockdale Hospital
- Piedmont Walton Hospital
- Piedmont Heart Institute
- Piedmont Physicians
- Piedmont Clinic
- Piedmont Healthcare Foundation

Piedmont provides a wide variety of services including, but not limited to:

- Cancer
- Transplant
- Primary Care
- Neurology
- Women’s Services
- Brain Tumor
- Urology
- Emergency
- Bariatrics
- Breast Health
- Diabetes
- Imaging
- Radiology
- Orthopaedic
- Rehabilitation
- Respiratory
- Robotic Surgery
- Wound Care and Hyperbaric

About Piedmont

- Founded in 1905 by two physicians
- Areas of clinical expertise include: cancer, heart, neuroscience, transplant and women’s services
- Serves the metro Atlanta area as well as communities in Fayette, Coweta, Henry, Newton, Pickens, Clarke, Rockdale, Walton, Muscogee (and surrounding) counties
- Named to AJC’s List of Top Work Places, 2016, 2017 & 2018
- AlwaySafe program: systemwide safety behaviors and prevention tools
- Epic: industry-leading EMR and practice management system provides better care by facilitating quality improvements and enhances the patient experience
About Community Medical Centers

Private, not-for-profit, locally-owned – $199 million in community benefit outreach
40+ years UCSF partnership on graduate medical education

Largest healthcare provider in California’s central San Joaquin Valley
- 1,129 licensed beds in 3 hospitals, inpatient behavioral health hospital and subacute care center
- 179,452 ER visits | 55,726 admissions | 9,621 babies born last year

Valley’s largest private employer
- 8,550 employees
- 1,400 affiliated physicians | 325 medical/dental residents

Serving 15,000-square-mile region

- Only Level 1 trauma and comprehensive burn center between Los Angeles and San Francisco
- Level 3 NICU and high-risk birthing center serves 5-county region

with unique health challenges

- Concentrated poverty – more than 35% of children live in poverty
- 100+ languages spoken, 43% adults don’t speak English well
- Higher than Calif. average rates for obesity, diabetes, lung disease and asthma
- 48% of population on Medi-Cal (Medicaid)
- 10% of Fresno County babies born premature – higher than some third world countries
- Lowest doctor-to-patient ratios in Calif.
Community Medical Centers highlights

- Founded in 1897 in when doctors joined with successful boarding house
- Becker’s Top 150 Places to Work in Healthcare list & Advisory Board’s Workplace of the Year 3x
- 3-year Health Ethics Trust certification for our compliance and ethics.
- GetWell Network’s national Leadership and Overall Achievement Awards
- Epic EMR integration throughout CMC, connecting more than 1,000 private physicians in region
- 9 consecutive Healthgrades’ Outstanding Patient Experience Awards to Fresno Heart & Surgical
- 3 consecutive Beacon Awards for Critical Care Nursing
- Top Performer Distinctions on Key Quality Measures by the Joint Commission for two hospitals & Advanced Stroke certification for another hospital
- Among 2 of 5 hospitals in California with Perinatal Certification for best practices and outcomes for mothers and babies

Community Medical Centers
Facilities & Affiliations
Healthcare Compliance Zones of Risk

We all are aware and have many and on the risks in healthcare related to:

Patient Quality and Safety!

We will move on to other business risks.................

Top Zones of Risk
# 1 - Causing you a Lack of Sleep?
Cybersecurity - Information Privacy & Security Compliance Audits
Cybersecurity
Protecting the most Vulnerable - Overview

• Information Security – By Definition
• The Case for Change
  • In the News …
  • Wishful Thinking?

• Knowing Your Cybersecurity Landscape
  • Digital Eco-System
  • Understanding the existing Cybersecurity Portfolio

Information Security – By Definition

• Information Security is the process by which an organization protects information and its critical elements including the systems, media, and people, along with the facilities that process, store and transmit that information.

  • In Healthcare: Enable and not disable empowerment of information for doctors and staff first.
Creating a Resilient Cyber Environment

- Protecting everything is not only impractical it’s financially not feasible for most organizations.
- Focus on the basics first.
  - Patch Management
  - Access Management
  - Valid Backups
  - Are existing logs being monitored on the Firewalls, Backups, Anti-virus reporting, CPU surges, others?
- What environment can be developed to withstand attack?

Knowing Your Cybersecurity Landscape

- Digital Eco-System
  - Thinking Locally and Globally
  - Sharing Threat Information in our community
  - We are electrons apart from bad actors not miles

- Understanding the existing Cybersecurity Portfolio
  - What are the Existing Protections?
  - Are the existing Cybersecurity Assets in a Healthy State?
  - What’s missing from the Portfolio?
SIEM
(Security Information and Event management)

- The segment of security management that deals with real-time monitoring, correlation of events, notifications and console views

- Log management aggregates data from many sources, including network, security, servers, databases, applications, providing the ability to consolidate monitored data to help avoid missing crucial events.
SIEM- Components

- **Data aggregation**: Log management aggregates data from many sources, including network, security, servers, databases, applications, providing the ability to consolidate monitored data to help avoid missing crucial events.

- **Correlation**: looks for common attributes, and links events together into meaningful bundles. This technology provides the ability to perform a variety of correlation techniques to integrate different sources, in order to turn data into useful information. Correlation is typically a function of the Security Event Management portion of a full SIEM solution.

- **Alerting**: the automated analysis of correlated events and production of alerts, to notify recipients of immediate issues. Alerting can be to a dashboard, or sent via third party channels such as email.

- **Dashboards**: Tools can take event data and turn it into informational charts to assist in seeing patterns, or identifying activity that is not forming a standard pattern.

- **Compliance**: Applications can be employed to automate the gathering of compliance data, producing reports that adapt to existing security, governance and auditing processes.

- **Retention**: employing long-term storage of historical data to facilitate correlation of data over time, and to provide the retention necessary for compliance and eDiscovery requirements. Long term log data retention is critical in forensic investigations as it is unlikely that discovery of a network breach will be at the time of the breach occurring.

- **Forensic analysis**: The ability to search across logs on different nodes and time periods based on specific criteria. This mitigates having to aggregate log information in your head or having to search through thousands and thousands of logs.

Protecting the MOST VALUABLE...!

- **Determine the mission critical systems**
  - EPIC/Cerner, PACS, the Network, Telephone Systems, Lawson/PeopleSoft, HVAC
    - Protect
    - Monitor
    - Vulnerability Identification and Remediation
    - Focus your efforts and have the highest security standards enforced

  - Build out from the center of Patient Care, Revenue Cycle and Infrastructure as one example
"Most Valuable Attack Vectors"

Some Common Threat Vectors
- Phishing
- Social Engineering
- Denial of Access
- USB Drop Attack
- Spoofing Attack
- Wireless Attack
- Malware Infection
- Web Server Attack
- Denial Of Service

The Most Valuable
- Bio-Med
- Epic Cerner
- Lawson Peoplesoft
- Databases
- Network Files

Data Leakage
- Data Leaks to DarkNet

Security Monitoring – Monitor and detect cyber threats
Data Loss Prevention (DLP) – Detect and prevent data leakage
Secure Network Resources – prevents unauthorized access to CMC data
Identity and Access Management - Improve access administration and privileges to CMC data

Other Considerations...

- Exclude whole regions of the world who you do not do business with
  - Have a process for doctors without borders, be reasonable.

- Have your Cybersecurity Portfolio “test attacked” by an independent group

- Go on the offensive and become hunters on your own network
Solution Functionality Overview (1 of 3)

QRadar SIEM (Security Information and Event management)

- Advanced management and correlation of logs and flows
- Thousands of built in security rules out of the box
- Thousands of pre configured, out of the box log sources
- Out of the box integration capabilities into a vast array of both IBM’s and other vendor’s security products (i.e. Symantec DLP)
- Single pane of glass for management and monitoring of potential security threats and vulnerabilities
- QFlow analysis for deep layer 7 packet visibility into security events
- Network behavior and anomaly detection
- Over 1,700 customizable, out of the box compliance reports
- The ability to bring third party threat feeds into QRadar

Solution Functionality Overview (2 of 3)

Vulnerability Manager and Scanner

- Helps prevent security breaches by discovering and highlighting high-risk vulnerabilities from a single integrated dashboard
- Conduct rapid network scans – periodically or dynamically to find security weaknesses and minimize risks
- Automate regulatory compliance with collection, correlation and reporting

IBM Premium X-Force Security Feed

- X-Force enrich QRadar threat analysis capabilities with up-to-the-minute data on threats
- Leverage the additional threat context provided by IBM Security X-Force Threat Intelligence to gain deeper insight and greater protection
Solution Functionality Overview (3 of 3)

Risk Manager

- Visualize current and potential network traffic patterns with network topology model based on security device configurations
- Quantify and prioritize risk with a policy engine that correlates network topology, asset vulnerabilities, and actual network traffic enabling risk-based remediation and facilitating compliance
- Centralize network security device management to help reduce configuration errors and simplify monitoring of firewall performance

Incident Forensics and IF Packet Capture

- Investigate security incidents using full packets captured from across CMC’s network
- Integrate with QRadar to decode, index, reconstruct, and analyze data
- Generate multiple views of data including relationships, timelines, source and threat category
- Helps resolve identified incidents in minutes or hours instead of days or weeks

NIST Cybersecurity Framework

<table>
<thead>
<tr>
<th>Category</th>
<th>Framework</th>
<th>ID</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>Information Assurance</td>
<td>A.10.2</td>
<td>NIST SP 800-53r3</td>
</tr>
<tr>
<td></td>
<td>Risk Analysis</td>
<td>A.10.3</td>
<td>NIST SP 800-53r3</td>
</tr>
<tr>
<td></td>
<td>Risk Management</td>
<td>B.6.1</td>
<td>NIST SP 800-53r3</td>
</tr>
<tr>
<td></td>
<td>Access Control</td>
<td>C.3.1</td>
<td>NIST SP 800-53r3</td>
</tr>
<tr>
<td></td>
<td>Awareness and Training</td>
<td>D.1.2</td>
<td>NIST SP 800-53r3</td>
</tr>
<tr>
<td></td>
<td>Data Security</td>
<td>E.1.1</td>
<td>NIST SP 800-53r3</td>
</tr>
<tr>
<td></td>
<td>Information Protection</td>
<td>E.1.2</td>
<td>NIST SP 800-53r3</td>
</tr>
<tr>
<td></td>
<td>Processes &amp; Procedures</td>
<td>E.1.3</td>
<td>NIST SP 800-53r3</td>
</tr>
<tr>
<td></td>
<td>Maintenance</td>
<td>E.1.4</td>
<td>NIST SP 800-53r3</td>
</tr>
<tr>
<td></td>
<td>Protective Technology</td>
<td>F.1.1</td>
<td>NIST SP 800-53r3</td>
</tr>
<tr>
<td>Detect</td>
<td>Anomalies and Events</td>
<td>G.1.1</td>
<td>NIST SP 800-53r3</td>
</tr>
<tr>
<td></td>
<td>Continuous Monitoring</td>
<td>G.1.2</td>
<td>NIST SP 800-53r3</td>
</tr>
<tr>
<td></td>
<td>Detection Processes</td>
<td>G.1.3</td>
<td>NIST SP 800-53r3</td>
</tr>
<tr>
<td>Respond</td>
<td>Response Planning</td>
<td>H.1.1</td>
<td>NIST SP 800-53r3</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
<td>H.1.2</td>
<td>NIST SP 800-53r3</td>
</tr>
<tr>
<td></td>
<td>Analysis</td>
<td>H.1.3</td>
<td>NIST SP 800-53r3</td>
</tr>
<tr>
<td></td>
<td>Mitigation</td>
<td>H.1.4</td>
<td>NIST SP 800-53r3</td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
<td>H.1.5</td>
<td>NIST SP 800-53r3</td>
</tr>
<tr>
<td>Recover</td>
<td>Recovery Planning</td>
<td>I.1.1</td>
<td>NIST SP 800-53r3</td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
<td>I.1.2</td>
<td>NIST SP 800-53r3</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
<td>I.1.3</td>
<td>NIST SP 800-53r3</td>
</tr>
<tr>
<td></td>
<td>Mitigation</td>
<td>I.1.4</td>
<td>NIST SP 800-53r3</td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
<td>I.1.5</td>
<td>NIST SP 800-53r3</td>
</tr>
</tbody>
</table>
Training and Awareness for Phishing

Think you’ve been Phished? Click me

• Don’t open email from senders you don’t recognize!
• Don’t open attachments without verifying the source!
• Don’t click on links in emails if you are not sure where it came from!

Teach employees to R.A.T. out bad emails:

R – Report suspicious emails by clicking on the “Report Phishing” button
in Outlook or by forwarding them to security.concords@piedmont.org.
A – Assume emails prompting you for information you would not
otherwise share are suspicious.
T – Take time to spot Piedmont Communication from fake.

Top Risks

• Bio-MED outdated devices
• Artificial Intelligence
• Account Management and Access Management Weakness
• Employees Responding to Phishing Attacks
• Risk Management Response to Cybersecurity Issues
• Vulnerability Management
• Asset Management
• Software Management
• Patching
• HVAC System Access
• Vendor Managed Software
• Information Security Policies
• Use of Terminology – Observation, Incident, Event

Only Use The Word Breach Once It Has Been Confirmed
ISACA Maturity Definitions

<table>
<thead>
<tr>
<th>LEVEL 1</th>
<th>LEVEL 2</th>
<th>LEVEL 3</th>
<th>LEVEL 4</th>
<th>LEVEL 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>PERFORMED</td>
<td>MANAGED</td>
<td>DEFINED</td>
<td>QUANTITATIVELY MANAGED</td>
<td>OPTIMIZED</td>
</tr>
<tr>
<td>General personnel capabilities may be performed by an individual, but are not well defined</td>
<td>Personnel capabilities achieved consistently within subsets of the organization, but inconsistent across the entire organization</td>
<td>Roles and responsibilities are identified, assigned, and trained across the organization</td>
<td>Achievement and performance of personnel practices are structured, measured, and evaluated</td>
<td>Proactive performance improvement and measuring based on organizational changes and lessons learned (internal &amp; external)</td>
</tr>
<tr>
<td>General process capabilities may be performed by an individual, but are not well defined</td>
<td>Adequate procedures documented within a subset of the organization</td>
<td>Organizational policies and procedures are defined and standardized. Policies and procedures support the organizational strategy</td>
<td>Policy compliance is measured and enforced</td>
<td>Policies and procedures are updated based on organizational changes and lessons learned (internal &amp; external) are captured</td>
</tr>
<tr>
<td>General technical mechanisms are in place and may be used by an individual</td>
<td>Technical mechanisms are formally identified and defined by a subset of the organization; technical requirements in place</td>
<td>Purpose and intent is defined (right technology, adequately deployed). Proper technology is implemented in each subset of the organization</td>
<td>Effectiveness of technical mechanisms is predicted, measured, and evaluated</td>
<td>Technical mechanisms are proactively improved based on organizational changes and lessons learned (internal &amp; external)</td>
</tr>
</tbody>
</table>

Top Zones of Risk

# 2 - Causing you Loss of Hair?

Revenue Cycle
Registration, Insurance Verification and Eligibility

How are you screening, monitoring and documenting Medicare Secondary Payer?
Are you one of the lucky hospitals being audited for Medicare Secondary Payer?

Coding, Charge Capture and Claims
Claims Transmission and Payment Posting

- Review the claims transmission process to evaluate how errors are addressed and what overrides can occur.

- How are payment postings monitored?

IRS Form 8300

How are you defining two or more related transactions to trigger the filing of Form 8300?

How are you monitoring this and over what period of time?

Review adjustments to accounts to verify that reversals are appropriately posted and major categories such as charity care adjustments are correctly stated.

- Accounts Receivable
- Denial Management
- Follow-up
- Collections
Top Zones of Risk
# 3 – Stress Eating

PEOPLE

People Compliance?

Paid Holidays  Fraternization  Safety
Firing
Unemployment Claims  Compensation  Harassment
Lawsuits
Bullying
Retention
Personal Leave/FMLA
Increasing Benefits Costs
Having Employees brings these issues to your Business
Affordable Health Care
Violence
Uncontrolled Labor Costs

Dress Code
Unplanned Time Off
Workers Compensation
Skills Training
Hiring
Overtime Costs
Safety
Complaints
Human Resources

Human Resources Operational Functions

<table>
<thead>
<tr>
<th>Procure</th>
<th>Develop</th>
<th>Compensate</th>
<th>Integrate</th>
<th>Maintain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Analysis</td>
<td>Performance Appraisal</td>
<td>Evaluation</td>
<td>Labor Relations</td>
<td>Health &amp; Safety</td>
</tr>
<tr>
<td>Recruitment</td>
<td>Appraisal</td>
<td>Wages &amp; Salary</td>
<td>Relations</td>
<td>Risk Management</td>
</tr>
<tr>
<td>Selection</td>
<td>Training</td>
<td>Bonus &amp; Incentives</td>
<td>Motivation</td>
<td>Social Security</td>
</tr>
<tr>
<td>Placement</td>
<td>Career Planning</td>
<td>Payroll</td>
<td>Grievance</td>
<td>Welfare</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Development</td>
<td></td>
<td>Discipline</td>
<td>Record Keeping</td>
</tr>
<tr>
<td>Transfer</td>
<td>Transition Planning</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Promotion</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

People Challenges

HR DEPARTMENT DILEMMAS
What HR Works on Most
- Handling employee disputes: 28%
- Dealing with issues: 16%
- Resolving new employee issues: 16%
- Training employees: 14%
- Managing employee benefits: 14%
- Approving vacation time: 10%
- Tracking sick and personal days: 8%
- Processing payroll: 7%

HR Complaints: 24%

HR EXPECTATIONS
What HR Does
- Handling employees disputes: 76%
- Dealing with issues: 72%
- Resolving new employee issues: 61%
- Training employees: 50%
- Managing employee benefits: 50%
- Approving vacation time: 48%
- Tracking sick and personal days: 48%

What Employees Expect
- Handling employees disputes: 76%
- Dealing with issues: 76%
- Resolving new employee issues: 68%
- Training employees: 55%
- Managing employee benefits: 54%
- Approving vacation time: 33%
- Tracking sick and personal days: 29%

Source: Survey of 500 employees and over 40 HR specialists
People Monitoring

Building Respect In The Workplace

Labor Laws

- Wage & Hour
- Job discrimination
- Overtime/minimum wage
- Family leave
- Age discrimination
- Disability discrimination
- Gender-pay differences

- Military Leave
- Worker’s Compensation
- Workplace safety & health
- Employee Benefit Security
- Unions & Their Members
- Employee Protection
Business risks facing an organization can be wide-ranging and diverse. The ultimate business risk any organization faces is the risk that it seizes to be a going concern. Business risks therefore comprise any factors that may contribute towards business failure.

- Loss of customers
- Increase in production costs
- Cash flow problems
- Decline in product demand
- Litigations and claims
- Technological obsolescence
- Increase in market competition
- Decrease in profitability
- Political and economic instability
- Over trading
- Inadequate financing
- High financial risk
- Risk of fraud and theft
- Increased regulatory enforcement

Other Top Zones of Risk
BUSINESS Headaches

Comments and Questions