Crowe Horwath

CHAN Healthcare™
A subsidiary of Crowe Horwath LLP

Internal Control Imperatives for Healthcare Leadership

Crowe® Healthcare Webinar Series

Learning Objectives

As a result of participating in this session, you should be able to:

- Recognize key risks and their potential impact to your organization
- Describe core operational and technology controls necessary to mitigate risks in the areas of:
  - Management training and accountability
  - Third party relationships
  - Cybersecurity threats and
  - Process automation
- Identify proven solutions for successful risk management

Management Training and Accountability

Across CHAN Healthcare, we perform in excess of 1,300 internal audits each year, covering:

- Information Technology
- Hospital Operations
- Coding
- Clinical Areas
- Financial Operations

One of the top three causes in our audit findings is the area of Management Training and Accountability

Polling Question #1

What percent of managers have never had formal training on “being a manager”?

A. 18%
B. 25%
C. 43%
D. 58%

Management Training and Accountability

CareerBuilder Survey of 3,910 Managers (2011):

- **58% say that they didn't receive any management training**
- 26% say that they weren't ready to become a manager when they became one

Management Training and Accountability

Key characteristics leading to promotion of Clinical Managers include:

- Strong technical healthcare skills
- Good patient satisfaction
- Respect of peers

BUT, many lack training in being business leaders

Management Training and Accountability

Example of required business leadership skills in an ancillary hospital department:

- Management of IT applications
- Privacy and security roles
- Payment card processing
- Business financial oversight (gross and net revenue, accruals)
- Human resources (performance evaluation, interviewing, productivity and conflicts)
- Strategy (business proformas, capital planning)
- Vendor management
- Budgeting
- Risk management

Management Training and Accountability

- Accountability
  - How Executive and Departmental Management take responsibility and oversee their function
  - How commitments are measured, monitored and reported for progress towards goals and accomplishments
  - How Management reacts when things go wrong to rectify atypical results

When oversight is lacking, processes are at higher risk for failure to achieve business strategy and objectives

Management Training and Accountability

Source: Copyright 2005-2010 National Center for Healthcare Leadership – Health Leadership Competency Model

Management Training and Accountability

A strong healthcare organization has:

- Strategic goals for each service
- Definition of manager's responsibility for achieving goals
- Strategic measurements, scoreboards, dashboards and monitoring tools
- Training needs assessment
- Management training/"Emerging Leaders" programs"
- Job descriptions defining leadership expectations
- Oversight at all levels of the organization

Trust but verify!

Third Party Relationships and Risk Management

- Today, healthcare organizations rely on a complex network of external service providers, distributors, partners and other entities
- Third parties pose significant risks related to regulatory scrutiny, cost pressures, compliance issues, data privacy and the organization's overall reputation
- While most organizations are concerned about their vulnerability to Third Party risks, a majority indicate devoting <20% of their internal audit resources in this area

Polling Question #2

Does your organization have an established Third Party Risk Management program?

- A) Yes, we have a mature Third Party Risk Management program
- B) Kind of, though it is informal and fragmented
- C) No, we do not have a Third Party Risk Management program
- D) I know who to email when something goes wrong

Third Party Compliance Issues in the News

- Anti-Kickback Statute Violation: Hospitals paid business associates to assist at clinics with translation, that then referred OB patients to the hospital

Posted: 6:29 p.m. Thursday, Aug. 7, 2014

Two plead guilty in massive Medicaid scam

Email 15 | Share 30 | Tweet 11 | ShareThis 156

Related

Atlanta

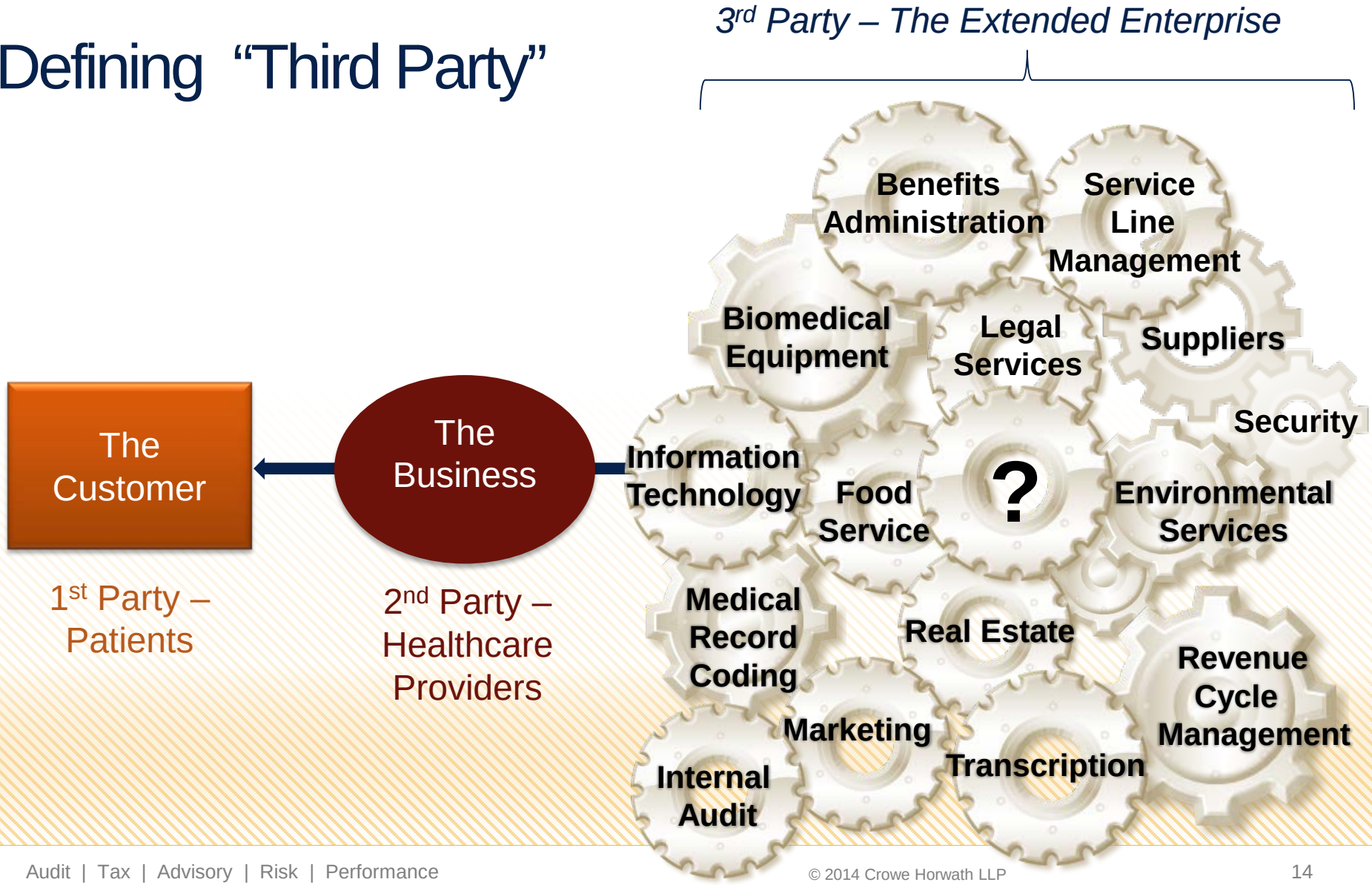
By Michelle E. Shaw

The Atlanta Journal-Constitution

Two people have pleaded guilty to receiving money for Medicaid-related patient referrals to hospitals in Atlanta and on Hilton Head Island, S.C.

Tracey Cota, 50, of Dunwoody, and Gary Lang, 58, of Atlanta, both admitted to conspiracy to violate the Anti-Kickback Statute

Defining "Third Party"



Why you should be concerned about Third Party risks:

- Non-compliance with laws and regulations
  - Health Insurance Portability and Accountability Act (HIPAA)
  - American Recovery and Reinvestment Act of 2009
  - Emergency Medical Treatment and Active Labor Act (EMTALA)
  - Anti-Kickback Statute
  - False Claims Act
- Financial loss and overpayment
  - Overbilling for services
  - Financial failure of a Third Party

Why you should be concerned (continued):

- Operational/Delivery/Quality Issues
  - Third Party does not deliver as promised, impacting operations
    - **Example:** Environmental and Nutritional Services Outsourcing – Quality Standards
- Technology and Security Risks
  - Third Party suffers a breach, resulting in data disclosure
    - **Example:** Recent breaches in Electronic Medical Records
  - New risks related to smartphones, tablets, social media and cloud computing
- Reputational Impact on your Brand
  - Third Party does not appropriately represent your organization and its values
    - **Example:** Not for profit hospital outsources collections to a vendor who engages in “extraordinary debt collection practices”

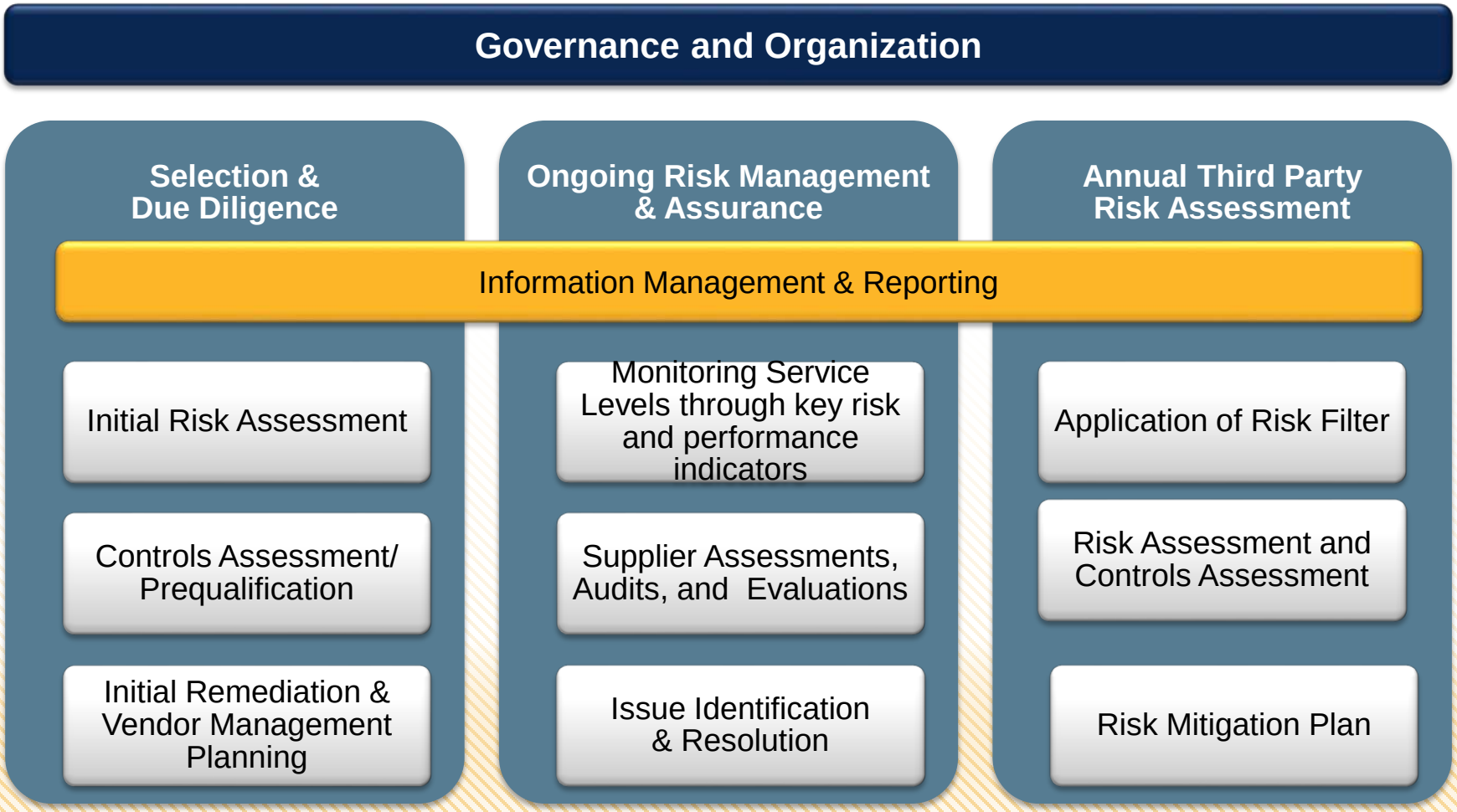
Third Party Risk Management Program

- Establish Ownership and Buy-in
  - Cross-functional coordination, executive leadership and oversight and clear goals are required
- Evaluate Third Party Risk Universe
  - Developing a comprehensive risk landscape is necessary to avoid a one-size-fits-all approach
  - Once you understand an Organization's risk profile, you'll be able to focus efforts on areas that present the highest potential risk, as well as reward

Third Party Risk Management Program

- Audit, Monitor, and Assess
  - Third Party Risk Management program should encompass
    - Risk measurement and monitoring
    - Performance measurement and monitoring
    - Benchmarking of performance and costs
    - Incident tracking
    - Evaluation of the value received from the relationship
  - Service organization auditor evaluation of Third Party controls

Third Party Risk Management Program Map

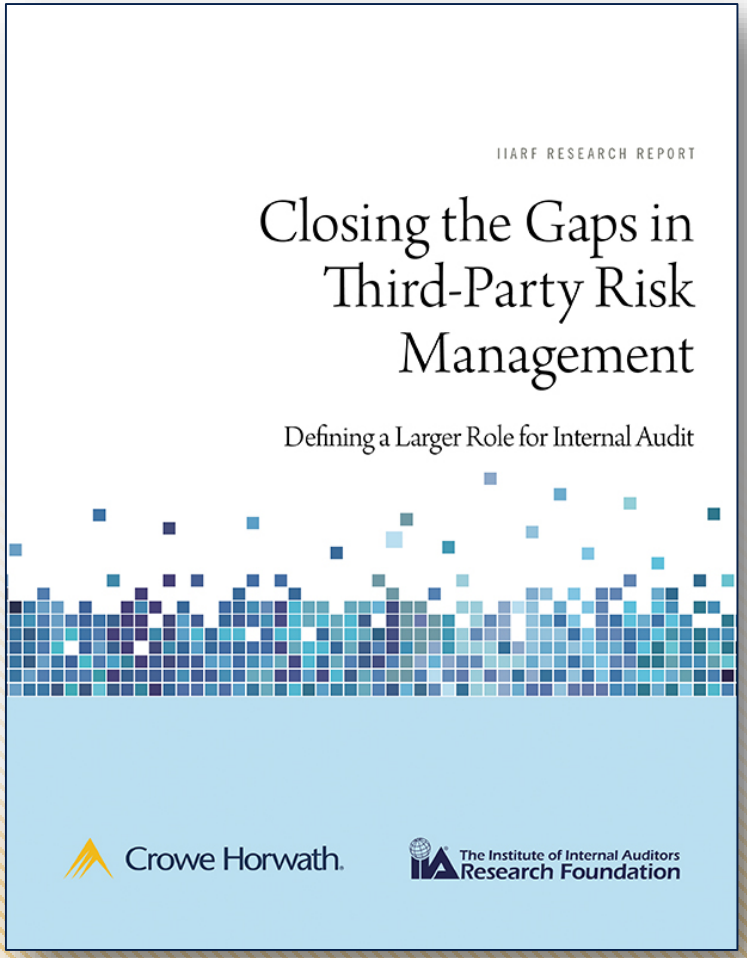


Internal Audit's Role in Third Party Risk Management

- Internal Audit can add value by assessing risk around the organization's business relationships
  - Assist Management with identifying the Third Party risk universe and risk rankings
  - Enhance Management's understanding of how Third Parties comply with regulations or policies that should be in place
  - Compare Third Party risk management approach with those used in the Organization's Enterprise Risk Management program
  - Confirm that service-level agreements are being met
  - Evaluate Statement of Standards for Attestation Engagement No. 16 (SSAE-16)
  - Provide consultation as contracts are being developed with Third Parties

IIARF Study

- What are the risks?
- What is IA's role?
- Where is IA involved today?
- Where is IA adding value?
- http://www.crowehorwath.com/insights/closing-gaps-third-party-risk-mang/



Cybersecurity and Threat Management

- Definition
  - “Cybersecurity encompasses a broad range of practices, tools and concepts related closely to those of information and operational technology security. Cybersecurity is distinctive in its inclusion of the offensive use of information technology to attack adversaries.”
  - More simply: Using resources to proactively protect systems and data from unauthorized access

Cybersecurity Impacts

- Privacy and Security Breach
  - Tremendous and varied impact
    - Regulatory, legal (criminal and civil, organizations and individuals)
    - Reputational
    - Financial
    - Patient Care
- Fraud and Identity Theft
  - Access and misuse Protected Health Information, Social Security Numbers, Credit Card Information
    - Internally or externally driven
    - Increased targeting of health information

Recent Health Breaches

1

Escalation of Breach Incidents

- Ponemon Institute indicates 90% of healthcare organizations had exposed their patients' data—or had it stolen—in 2012 and 2013
- Washington Post - since federal reporting requirements kicked in, US Department of Health and Human Services has tracked 944 incidents involving 30.1 Million people
  - Theft – 17.4 Million
  - Data Loss – 7.2 Million
  - Hacking – 3.6 Million
  - Unauthorized Access – 1.9 Million
- Not if, but when…

Breach – Cause and Impact

- 42% malicious or criminally motivated, 29% system issues, 30% related to human error
  - Lost or stolen devices
  - Hacking, phishing
  - Business partners out of compliance
  - Inappropriate disposal/handling of PHI (printers, trash/dumpster)

- HITECH increases potential fines and penalties for a breach
  - Price tag ranges from $50,000 to $1.5 Million per violation
  - Average breach cost to healthcare is $316/record vs. $201/record for other industries
  - Estimated cost to the industry - $5.6 Billion/Year

Fraud and Identity Theft

- Data breach does not necessarily result in Identity theft, but…
  - 25% of people who received a data breach notice eventually were victims (Javelin Strategy and Research)
- Healthcare data is valuable – and criminals want it
  - PhishLabs says stolen health credentials are worth between 10 and 20 times more than a credit card number
  - Credit.com – “Nearly half of identity thefts involve medical data” (43%)
- Damage to individuals
  - Credit ratings
  - Insurance benefits
  - Mingling of medical records with another individual – improper care (wrong blood type, invalid health history)

Polling Question #3

According to a Health Information Management Systems Society (HIMSS) Survey in 2013, about 69 percent of health security professionals said their organization had a data breach plan in place, and another 27% were developing a strategy. Where do you feel your organization stands in addressing breach risks:

- A) have a fully defined and implemented breach plan
- B) data breach plan is developed, but not fully implemented
- C) plan is not yet developed
- D) unknown

Cybersecurity Threat Management – Strategies

- Cybersecurity Framework
  - Leverage available guidance and expertise
    - National Institute of Standards and Technology (NIST)
    - Internal and external partners – gap analysis and plan to address
- Data Loss Prevention
  - Know your data and related risks – the only way to effectively manage!
    - Data classification programs are key
  - Establish, implement program of controls based on risks
    - Periodically test standards and barriers (network, operating system, application, mobile environment)
      - “No surprises” validation of controls

Cybersecurity Threat Management – Strategies

- Raise Security Awareness
  - Cross organizational and functional training and threat communication
  - Addresses human element through education on risks and leading practices

- Update/Maintain Systems (network, Operating System, applications, devices)
  - Ongoing threat assessment and analysis
    - What is the vulnerability
    - System-specific impact
    - Timely implementation for critical updates
  - Patch management – proactively correct known vulnerabilities
    - Office of Civil Rights fined Alaskan Mental Health Provider for failure to patch – HIPAA violation

Cybersecurity Threat Management – Strategies (continued)

- Monitor and Respond
  - Vulnerability assessment
    - Current threats, susceptibility - internal/external
  - Activity monitoring
    - Propriety of both system and transaction level actions
  - Intrusion detection and incident response
    - Timely identification, mitigate risk and impact, and evidence diligence

Process Automation Risks

- Greater reliance on technology = greater risk
  - HITECH, Affordable Care Act - EHRs, Health Information Exchanges, Telehealth
- Confidentiality, Integrity and Availability of Information
  - Security and access management
  - System and data change management
  - Business continuity and disaster recovery
- Pervasive impacts from weak or absent controls
  - Financial
  - Legal/Regulatory
  - Reputational
  - Worst case – patient care

Process Automation - Impacts

- Confidentiality/Integrity/Availability - Impacts
  - Failure to meet minimum necessary (HIPAA regulatory)
  - Inability to process credit payments (PCI DSS compliance)
  - Systems fail and can't be recovered
    - Risks increase with passage of time since implementation of EHR
  - Patient given wrong/harmful care – drug interactions, surgery errors
    - Alert overload results in failure to identify and act on critical alerts
    - Failure to design controls to protect against errors – edits and validation checks
  - Incorrect charges for procedures due to invalid data
    - Cut and paste/cloning in EHRs may result in documentation errors
    - Payment and audit impact (recoupment, penalties, Corporate Integrity Agreements)
  - Incorrect submission of required quality data

IT General Controls – Foundational Solutions

- Identity and Access Management
  - Access authorization and removal, login and password management, role based access, periodic verification of access (re-certification)
- Logging and Monitoring
  - Define what needs to be monitored, configure logging to capture desired activity, and review activity for propriety (system and data)
- Change Management
  - Programs, data, interfaces
  - Program management practices, testing and user engagement, training, monitoring and error resolution
    - No surprises, systems and data can be relied upon
    - Meaningful Use impact if training and user engagement are lacking (dollar and quality impacts)

Foundational IT Controls

- Business Continuity and Disaster Recovery
  - IT and organization collaboration to define needs and priorities
  - Communication is critical to success

- IT Governance
  - Oversight and direction, support for key initiatives
    - IT as a service provider – clear roles and accountability
    - Funding and resource roadblocks
    - Corporate/clinical engagement

Foundational IT Controls (continued)

- "Shadow IT" – systems and solutions developed/supported outside of IT
  - If acquired without IT engagement/input, increased risks
    - Business does not understand the impact of the system security design/requirements
    - Hybrid systems may cause unclear accountability – who manages – Vendor, Department, IT?
  - Engage IT up front in risk assessment and acquisition
    - Define and identify needed mitigating controls
    - Clarify accountability for controls over security, backup, change management

Polling Question #4

We've established that foundational IT controls are essential to preserving the confidentiality, integrity and reliability of healthcare systems and information. What do you feel is the greatest challenge to your organization's ability to implement and sustain technology controls:

- A) lack of corporate leadership support and/or governance for IT
- B) lack of expertise – gaps in the number and availability of knowledgeable resources to execute control processes
- C) funding gaps – failure to invest capital and operating funds to support core programs
- D) competing initiatives – prioritization of critical initiatives gets in the way of the basics

Solutions for Success

- Strategy in Selecting New Leaders and Managers
- Management Must be Active in Managing Vendors (…and “outsourcing” risk)
- Internal Audit/Management and Governance Partnership
- Embrace Continuous Risk/Controls Assessment
  - Know weaknesses, mitigate risks, apply lessons learned
  - Leverage internal and external expertise

For more information, contact:

Sarah Cole
Direct (314) 802.2049
scole@chanllc.com

Eric Jolly
Direct (415) 438-5568
ejolly@chanllc.com

Janice Brotherton
Direct (602) 307-2164
jbrotherton@chanllc.com