HOW AND WHEN TO UTILIZE IT
INTERNAL AUDITORS IN COMPLIANCE
CHASE WHITAKER
HCA - HOSPITAL CORPORATION OF AMERICA

HCA
Hospital Corporation of America
$37B annual net revenue
$24B total assets
$7B EBITDA
$1.8B Net Income
215,000 employees
5% of US inpatient services
Common line of business, systems, and security model

HCA
FACILITIES AND LOCATIONS
Hospital Corporation of America
165 hospitals and 115 surgery centers located in 20 states and London
**WORKSHOP OBJECTIVES**

Using IT Audit Resources is No Longer Optional
- Understanding the basics of IT auditing

Building Your Annual Compliance Plan
- Identifying key areas where and how you can use IT auditors

Overseeing the Work of IT Auditors
- Tips for effectively managing assigned IT audit resources and the process
TYPICAL AUDIT PROCESS FLOW

FRAMEWORKS FOR INFORMATION TECHNOLOGY

COBIT
- Control Objectives for Information Technology
- IT governance framework issued by ISACA (free)
- Control objectives for safeguarding information assets

COSO
- Most widely used internal control framework (commonly used for SOX compliance)

ISO 17799 / 27001
- Detailed information security standards (commonly used to benchmark a company’s policies/standards)

ADDITIONAL FRAMEWORKS

NIST 800 Series
- U.S. federal government computer security policies, procedures, and guidelines

GAIT Methodology (Institute of Internal Auditors)
- Focused on IT general controls
TYPES OF IT AUDITS

Application Assessments - Cloud, internally-developed
IT Infrastructure - Operating System, Database, Network
IT Operations - Project Management, Change Management, Problem Management, Service Desk, Business Continuity, Vendor Management
Regulatory Compliance (SOX, HIPAA, HITECH/Meaningful Use)
Cybersecurity
Data Analytics and Continuous Auditing / Monitoring

COMMON IT AUDIT TESTING AREAS

User Access
- Generic User IDs
- Access matched with job function
- Process for communication and removal of terminated employee’s access

Password and Account Settings
- Account lockout threshold
- Password length
- Password complexity

COMMON IT TESTING AREAS – MEDIA DISPOSAL

How are retired hard drives disposed?
How is removable media disposed?
APPLICATION REVIEW SCOPE AREAS

Vendor Management
- Information Security Agreements (ISA)
- Business Associate Agreements (BAA)
- Service Level Agreements and monitoring (SLA)

Project Management
- Project charter
- Functional and non-functional requirements
- Project plans
- Issue management
- Project dependencies

APPLICATION REVIEW SCOPE AREAS

Usability
- End-user documentation
- User training
- Ease-of-use
- Reporting

Application Security
- Authentication (who are you?)
- Authorization (do you have the right level of access?)
- Password / PIN security
- Passwords sent in clear text

APPLICATION REVIEW SCOPE AREAS

Change Management
- Change control procedures
- QA/Test environments
- Segregation of duties
- Configuration management

Data Integrity & System Interfaces
- Input validation controls
- Masterfile management
- Alerting and monitoring
- Transaction balancing
- Failed transaction re-processing
CLOUD COMPUTING

Like many consumer offerings, many business solutions are migrating to cloud-based environment

Benefits:
- Quick time to market
- Access from anywhere with an Internet connection
- Often cheaper than hosting own infrastructure

LOGICAL SECURITY - OVERVIEW

- Logical security controls should ensure confidentiality, integrity, and availability over systems and data (CIA).
- Strong authentication controls should prevent user accounts from being compromised.
- Adequately restrict file shares to appropriate users.
- Apply patches and system updates timely.

LOGICAL SECURITY - RISKS

Authentication controls may not provide reasonable measures to protect against unauthorized access.
Excessive file shares may allow inappropriate access to sensitive data.
Outdated patches and virus updates may leave systems susceptible to:
  - Extended downtime
  - Viruses
  - Unauthorized access
  - Other malicious activity
LOGICAL SECURITY – RISKS (CONTINUED)
- Inadequate protection over sensitive data resulting in unintended disclosure.
- Unnecessary network services may be exploited to gain unauthorized access to sensitive data.

LOGICAL SECURITY – AUDIT TESTS
- Compare password controls to organizational standards or best practices.
- Review network file shares for appropriateness and necessity.
- Determine if sensitive data is encrypted within databases, on hard drives, and during network transmissions.
- Evaluate the process to apply patches/updates to the operating systems, databases and applications.
- Ensure anti-virus settings ensure definitions are up-to-date.

USER ACCESS - OVERVIEW
- Users and their system activity should be uniquely identifiable.
- User access requests, modifications, and removals should be documented and approved.
- Terminated users should have access removed timely.
- Access levels should be based on a user’s job duties (least privilege principle).
- Remote access should rely on secure protocols.
USER ACCESS – RISKS

- Undetected fraudulent/inappropriate use of critical systems and data
- Access granted without valid approval
- Access to critical systems and data by unauthorized users
- Appropriate access not defined for each specific job role (i.e., role-based security)
- Remote access to critical systems/data not configured correctly or using insecure protocols (e.g., modems, public networks)

USER ACCESS – AUDIT TESTS

- Ensure user administration procedures have been developed.
- Review system accounts to determine if any terminated employees/unauthorized users have active accounts.
- Evaluate user access, including administrator-level accounts, for adequacy and appropriateness based on the user’s job duties.
- Determine how remote access is granted, and recommend the replacement of insecure solutions.
- Ensure audit logging is enabled on critical systems/accounts and that logs are reviewed timely.

DISASTER RECOVERY/BUSINESS CONTINUITY - OVERVIEW

- Plans help minimize business impact in event of IT service interruption.
- Plans should be updated regularly and routinely tested to ensure systems and data can be recovered timely following a disaster or other interruption.
DISASTER RECOVERY/BUSINESS CONTINUITY - OVERVIEW

- Plans and data backups should be stored offsite for recovery needs.
- Quality of backup media and restoration tests should be periodically performed to ensure success of backup processes.

DISASTER RECOVERY/BUSINESS CONTINUITY – RISKS

- Backups may not include all necessary business data for comprehensive recovery in the event of unexpected system downtime or a disaster.
- Data may be compromised by unauthorized individuals due to improper securing of backup media.
- Extended downtime in the event of a disaster due to inadequate/lack of disaster recovery testing or thoroughly documented plans.
- Lack of executive/senior management support.
COMPLIANCE PROGRAM ADMINISTRATION

Compliance Program Governance
Policies & Procedures
Education & Awareness
Effective Communication

- Monitoring
- Auditing/Risk Assessment
- Investigation & Response To Detected Offenses
- Disciplinary Action

REGULATORY COMPLIANCE SIGNIFICANCE

- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry (PCI)
- Gramm-Leach-Bliley Act (GLBA)
- Centers for Medicare and Medicaid Services (CMS)
- ICD-9 ... or I10 ... or 9 ... OK, 10
- Sarbanes-Oxley (SOX)
IT AUDIT REGULATORY FOCUS

- HITECH Act - “Meaningful Use” of Certified Electronic Health Record Technology
- HIPAA - Privacy and Security of Protected Health Information
- Sarbanes-Oxley (SOX) - Financial Reporting
- Core Measures - “Pay for Performance”
- Payment Card Industry (PCI) - Credit Card Processing

LEVERAGING TECHNOLOGY

Organizational Compliance Related Activities Examples

- Billing Claims Scrubbing Software, Pre-Claims Submission
- Coding Accuracy Software Aids
- On-line Coding Education and Proficiency Testing Tools
- On-line Completion of Conflict of Interest Disclosures
- Automated Annual Signing of Confidentiality Agreement linked to Performance Evaluations
- Two-Midnight Rule
  - Who is minding the clock?
  - Hospital Medications - effects on Meaningful Use calculations

- ABN Software
- Laptop and USB Encryption Tools and Monitoring
- Confidential Data Leakage Detection/ Prevention Software Tools
- Data in Motion - Monitoring of emails, FTP, and other
- Patient Privacy - Applications Monitoring of User Access to patient records
LEVERAGING TECHNOLOGY

Compliance Department Administration Examples

- Compliance Issues / Investigations Tracking Database
- Monitoring of Eligible Professionals
- Audit Reports / Compliance Meeting Actions Follow-up Database
- Compliance Program Education
- Tracking database and/or on-line education
- Modules and/or tracking completion
- On-line subscription services and list-servs
- On-line web-based survey tools

---

LEVERAGING TECHNOLOGY

Compliance Department Administration Examples

- OIG-RATS-STATS Statistical Sampling Software
- Compliance staff with user access to key compliance-related information systems
- General compliance metrics / dashboard information for governance
- Contract administration for Compliance Program areas of responsibility (BAA’s, Physician Contracts)
- Compliance Auditing and Risk Assessment Knowledge Bases
THE “WHY?”

- More Effective Compliance Auditing and Monitoring
- Data analytical tools can facilitate 100% review of all transactions rather than samples.
- Number of records that can be imported and analyzed is limited only by hardware capabilities. >1 million records can be analyzed on high end PC.
- Sophisticated data analytical programs have “built-in” commands, functions, and filtering capabilities that enable rapid insights into data and potential issues.

THE “HOW?” – SOME TECHNIQUES

- SUMMARIZE - count records for each distinct value of selected character or date fields and subtotal numeric fields for each of these distinct values.
- STRATIFY - count the number of records falling into specified intervals (strata) of numeric field or expression values as well as to subtotal one or more fields for each stratum.
- CROSS-TABULATE - analyze character fields by setting them in rows and columns. By cross-tabulating character fields, various summaries, areas of interest, and subtotal numeric fields can be produced.
- DUPS OR GAPS - “Dups” detects whether key fields contain duplicate records AND “Gaps” detect gaps in the sequence of key fields.
THE “HOW?” – SOME TECHNIQUES (CONT.)

- RELATE TABLES - combine data from two or more tables as if they existed in a single table. Fields can be added from related tables to a view or use the Extract command to create new table of related fields.
- JOIN TABLES - combine fields from two tables into a third table. A separate table is needed requiring fields from two separate tables.
- EXTRACT - extract selected records or fields from the current table and copy to a different table.
- EXPORT - export data to another application (spreadsheets, databases, etc.).

THE “WHERE?” – DATA SOURCES

Revenue Cycle data (with focus on government payers)
- Medicare/Medicaid revenue by department or service area
- Medicare quality improvement PEPPER Reports
- Coding accuracy statistics and trends
- Utilization reports by DRG and CPT codes and by payor
- Physician billing
  - Medicare Development Letters
  - Workload RVUs per visit
  - Frequency Distributions of CPT Utilization

THE “WHERE?” – DATA SOURCES (CONT.)

Results of reviews by Medicare or other government reviewers
- Internal or external audits reports
- Other external reviews
  - Consultants reports
  - Feasibility studies
THE “WHERE?” – DATA SOURCES (CONT.)

Quality Reporting data and metrics
Patient Complaints - volume and nature
Patient and Employee Safety Occurrence Reporting
Compliance Hotline calls
  • by type, location
  • substantiated vs unsubstantiated
Patient / Physician / Employee Satisfaction Surveys
Survey results from Joint Commission, CMS or State Regulatory Agencies

COMMON HIT VENDORS & SYSTEMS

THE “WHEN?” TIMING FOR COMPLIANCE REVIEWS

Consider During Planning & Scoping Phases
  • Obtain data directly from key information systems and databases
  • Understand key data elements of population (e.g., Medicare Credit Balances) to provide for accurate analysis of business area and identify items that may represent risks or vulnerabilities
  • Direct system access by Compliance Department staff to the transactions Masterfile or data warehouse facilitates quicker and easier review of transactions.
A “Continuous Auditing and Fraud Detection” program may supplement traditional compliance and internal audit activities to more timely address business risks which could significantly impact the organization. Continuous Auditing is the periodic or regularly scheduled performance of various review techniques (automated or manually performed) designed to:

- detect unusual activity
- monitor key privacy, financial, and security controls
- test compliance with regulatory requirements
- and identify and mitigate other business risks before they have a significant adverse impact on the organization.

CONTINUOUS AUDITING / MONITORING EXAMPLES

- Emails with SSN’s or Personal Health Information blocked by email gateway filters
- Medicare Credit Balances
- Coding Software Edits by coder / physician / location
- Comparison of Terminated Employees lists to system access
- Claims Scrubber Reports and metrics
- Monthly checks of OIG/GSA exclusion Lists
- Transaction or event “alerts” based upon compliance criteria
- Comparison of data from timekeeping system to user access and transaction date and time stamps
COORDINATION WITH RISK MANAGEMENT

Enterprise Risk Management
- Compliance Risks
- Related IT systems & data
- IT Audits

NEW SYSTEMS IMPLEMENTATIONS

Participation by Internal Audit on multiple vetting and approval teams
- Monitor security risks
- Monitor compliance risks
- Understand technologies to be used
- Brainstorm possible audit approaches
- Control design input

Examples
- Patient Portals
- Health Information Exchanges
EMERGING IT RISKS – SOME ARE ALREADY HERE!

Cybersecurity
Patient Portals

Data Exposure
- Patients (SSN, PHI, credit cards)
- Intellectual Property (clinical trials, mergers & acquisitions)

Cloud solutions
- Procurement
- Customer Relationship Management (e.g., Salesforce.com)
- Email
- Dropbox, Box.com
- Amazon Services

EMERGING IT RISKS – SOME ARE ALREADY HERE!

Cloud solutions
- Pharmacy management and analytics
- Coding solutions
- Remote radiology

Internet-enabled medical devices
- Infusion pumps, CT, MRI, patient monitors
- Secure configuration and patching
- Organizational accountability

Multi-function devices (printer / copier / fax)
CLOUD COMPUTING RISKS – QUESTIONS TO ASK

Who owns data uploaded to the cloud?
Where will the data reside (e.g., within the U.S.)?
“Right to audit” clause in the contract?
Are enough dedicated resources (e.g., servers, CPU power, RAM) available to fulfill the business function?
How is business data destroyed once the contract ends?
Do service levels defined by the vendor meet your business requirements?

INFORMATION SYSTEMS AUDITS

Clinical Data Warehouse - all HCA clinical data into one central location
Patient encounters
Thousands of data elements for every patient
Company-wide analytics
HCA: 65 Petabytes and growing

HOW MUCH IS A PETABYTE OF DATA?

1 Petabyte = 1,000,000,000,000,000 (10^15) bytes
1 Petabyte = 1,000 Terabytes
1 Petabyte = 1,000,000 Gigabytes
1 Petabyte = 1,000,000,000 Megabytes
1 Petabyte = 1,000,000,000,000 Kilobytes
1 Petabyte ≈ 1.125 × 10^12 Gigabytes
1 Petabyte ≈ 1.125 × 10^15 Kilobytes

1 Petabyte is a lot of data.
CONTACT INFORMATION

Chase Whitaker
Director of Internal Audit
Chase.Whitaker@HCAHealthcare.com
Twitter: @43chase