HP 3.03: Maintaining Compliance in a Growing Environment

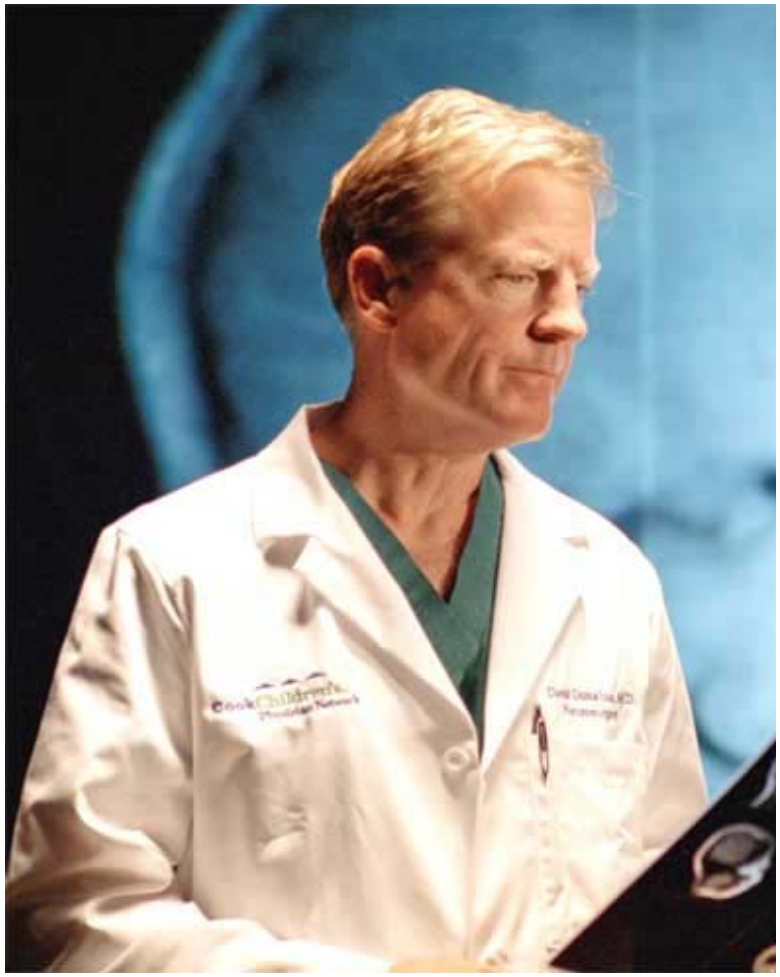
Jody S. Hawkins,
Information
Security Officer

Cook Children's

Topics To Cover

- Cook Children's
- The Structure of Security
- Plan for Growth
- Maintain Checks and Balances
- Accountability
- Cost and Convenience
- Setting Goals

Cook Children's



Cook Children's

Cook Children's Health Care System, based in Fort Worth, Texas is one of the country's leading integrated pediatric health care delivery organizations.

Cook Children's mission is to improve the health status of children through the prevention and treatment of illness, disease and injury.

CookChildren's℠

Cook Children's

The non-profit, exclusively pediatric organization is comprised of six companies:

- Cook Children's Health Care System - Integrated Management
- Cook Children's Medical Center - Inpatient Care, Outpatient Care
- Cook Children's Physician Network - Primary Care, Specialty Care
- Cook Children's Home Health - Home Care
- Cook Children's Health Plan - Insurance
- Cook Children's Health Foundation - Fund Raising

CookChildren's℠

Cook Children's



Cook Children's offers pediatric care in more than 30 pediatric services and specialties and operates more than 30 primary care pediatric locations, two urgent care centers, six outpatient clinic-based specialties in seven locations and 15 hospital-based specialties.

CookChildren's℠

The Structure of Security

- Reporting Structure
  - The Information Security Officer reports to the Corporate Compliance Officer and sits on the Corporate Compliance Committee
  - The Information Security Office, under the direction of the Information Security Officer, is a division of Internal Audit and oversight for the Information Security Office is provided by the Corporate Compliance Committee
- The diversity of environments within a Health Care System is great

The Structure of Security

- Data and Information Asset Owners – The Directors
  - Data Owner Representatives
    - Role Based Access Assignments
    - Data Retention Periods
    - Acceptable Use of Data
    - Data Classification
  - Information Asset Managers
    - Regular Inventory of Information Assets
    - Authorized usage of Assets
  - Information Security Delegates
    - Disseminate Information Security Awareness material
    - Perform regular audits and spot checks
    - Be the "Champion" for security in their area
  - Information Custodians
    - IS/IT staff
    - Provide technical assistance and oversight

CookChildren's

The Structure of Security

- Framework / Process Flow
  - Control
    - Perform Risk Assessment
    - Create Policy Statements
  - Planning
    - Develop process for implementation
    - Integrate Policy statements into existing or new policies
    - Create Training Materials
  - Implementation
    - Publish New Policies
    - Train Users
    - Outline Audit Criteria
  - Evaluation - Ongoing
    - Begin Audits
    - Investigate and Remediate
  - Maintenance
    - Review for Compliance and Pertinence
    - Start Back at Control or Schedule next Review

The Structure of Security

- Information Services Security Administration
  - IS Staff dedicated to information security tasks
  - Oversight provided by the Information Security Office
  - Assists the Information Security Office in performing regular audits and ensuring checks and balances are in place
  - Performs immediate functions of the Computer Emergency Response Team (CERT)
  - Ensures proper maintenance is performed
  - Audit results are given to the Information Security Office and those results are validated and included in the Information Security Score Formulas

Plan for Growth

- The Information Security Officer must stay aware of all initiatives of the organization
  - Early involvement makes for easier process
  - Needs to tailor the Information Security Program to the organization
    - Security Considerations Include:
      - Physical Security requirements
      - Data retention periods
      - Adequate logging
      - Space requirements for log files
      - New audit requirements
      - New policy and procedures
      - Resource requirements

CookChildren's

Plan for Growth

- The job of the Information Security Officer is to provide adequate information to Executive Leadership so proper decisions can be made
  - The information must be timely
    - Once decisions are made, it is difficult to go back and undo or redo the process
  - The information must be accurate
    - All information must be well researched and documented
  - The information must be non-biased
    - Base your findings on case studies, best business practices, and the law
  - The information must include remediation
    - Include information for an alternate solution

Cook Children's

Plan for Growth

- Keep your information up to date and well organized
  - Consolidate all Risk Assessments, Gap Analysis documentation, and Business Impact Analysis information for the entire organization
  - Consolidate all audit results, security investigations, and remediation results for the entire organization
    - Use this information to paint an overall security posture for the organization and base your recommendations, as much as possible, on observable data results rather than subjective experience

Plan for Growth

- Write Policies for approval with an extended implementation date
  - Solid policy that has time to go through an approval process will result in leadership approval and you will have a basis for future implementations
    - The approved policy can be used to write justification for increased staffing levels, budget approval, increased project prioritization, adherence to guidelines, etc.
- Keep the Information Security Program organized
  - Identify all policies, procedures, standards, and guidelines that relate to the security and privacy of information
  - Use Data and Information Asset Owners to identify areas that will need more attention
  - Include Information Security requirements in implementations early on

Maintain Checks and Balances

- You cannot allow the growing environment to outgrow your current initiatives
  - More employees means more users means more resources for audits
  - As policies and procedures are added or modified to keep up with the growing environment, so should audits be added or modified
    - More audits means more resources needed to ensure compliance
  - Information Services will grow rapidly with the organization

Maintain Checks and Balances

- Within Information Services
  - IS Security Administration Team
    - Information Security performs oversight and sets requirements
    - Information Services must increase the staffing of the IS Security Administration Team to keep up with the Information Security requirements
    - Make this an Administrative or System Wide Policy
      - Cook Children's defines this in a Corporate Compliance Policy that is set as an Administrative Policy

Accountability

- Information Security must have authority to audit and perform investigations and the ability to hold departments, areas, and individuals accountable for non-compliance with the Information Security Program
  - Cook Children's structure allows Information Security to raise concerns through the Corporate Compliance Program
  - All pertinent information is presented to Executive Leadership on a regular basis and areas that are not in compliance with the Information Security Program are identified

Accountability

- This must be a "top down" approach
  - Executive Leadership holds the Data and Information Asset Owners accountable for their departments
  - The Data and Information Asset Owners have the responsibility for their departments and hold their Data Owner Representatives, Information Asset Managers, and Information Security Delegates responsible for remediation of compliance issues

Accountability

- The Information Security Officer is held accountable for all instances where adequate information regarding an area of non-compliance was not escalated properly
  - The Information Security Officer holds the Information Security Office accountable for not performing adequate oversight
  - The Information Security Office reports all areas of non-compliance and specific non-compliance issues to the Information Security Officer who, in turn, reports this activity to the Corporate Compliance Committee to include in the Compliance Report

Cost and Convenience

- Another area of consideration is adequate software for a growing environment
  - Does your organization use "home grown" or "garage" software packages?
    - Does the software meet minimum security requirements?
    - Is the software robust enough for the size of the organization?
    - Is everything centralized within Information Services?
    - Is all data being backed up appropriately?
    - Are retention requirements being met?
    - Does the software allow for adequate logging?
    - Are the logs being kept in a centralized location?
    - Is adequate maintenance being provided?
    - Are user accounts being considered in the termination procedures?
    - And the list goes on…

Cost and Convenience

- Cheap software packages tend to leave gaping holes in security
  - Many cheap software packages provide no password protection or the ability to create individual accounts and leaves the organization at risk for repudiation of data and many are loaded on single workstations and are not backed up properly
- This may be fine for a small doctor's office with two computers and keeps everything in paper file; however, this is not alright large organizations
  - Only enterprise software solutions that are robust enough should be considered for use
    - Adequate security
    - Adequate logging
    - Adequate account provisioning
    - Centrally located within the organizations IT infrastructure
    - Backed up nightly
    - Considered when performing the Business Impact Analysis
    - Listed as an approved software
    - Licensing is maintained
    - Upgrades and patches stay current
    - Adequate audits are performed
    - Restrictions for data usage can be implemented
    - And the list, again, goes on

Cost and Convenience

- You can't have your cake and eat it too
  - Software that does not provide adequate security requires extremely inconvenient tasks that must be performed
    - Network folders can restrict access
    - Without adequate account provisioning and logging, the information must be printed, verified, signed, and scanned back in to the system if it is to be kept electronically
    - Manual backup to CD ROMs or other media must be performed if not centralized within IS
    - What about off-site storage?
    - What about retention, maintenance, upgrades, etc.?

Cost and Convenience

- This is a necessity, not convenience, in large organizations
  - Minimum application requirements need to be set and the Information Custodians for the Data and Information Asset Owners should be tasked with assuring all software that is being considered falls within those minimum standards
    - If there is a push to implement a software package that does not meet the minimum requirements then it would be escalated to Information Security
    - Information Security will include this non-compliance issue in the Compliance report and formal recommendations can be made

Setting Goals

- In the end, it is up to leadership to decide what direction to take. If leadership is continually provided with adequate information and the big picture stays in focus, then the Information Security Officer has done their job
- In preparing for future growth, you should keep security considerations visible
  - Risk often is accepted due to money, time, and available resources
  - Get leadership to commit to security goals early or commit to a future goal
    - Establish a multi year plan if necessary
    - Include security concerns with pending implementations

Q & A

CookChildren's