# "Auditing and Monitoring for HIPAA Compliance"

## HCCA COMPLIANCE INSTITUTE 2003

**April, 2003**


**Presented by:**

**Suzie Draper**

**Sheryl Vacca, CHC**

# The Elements of Corporate Compliance Program

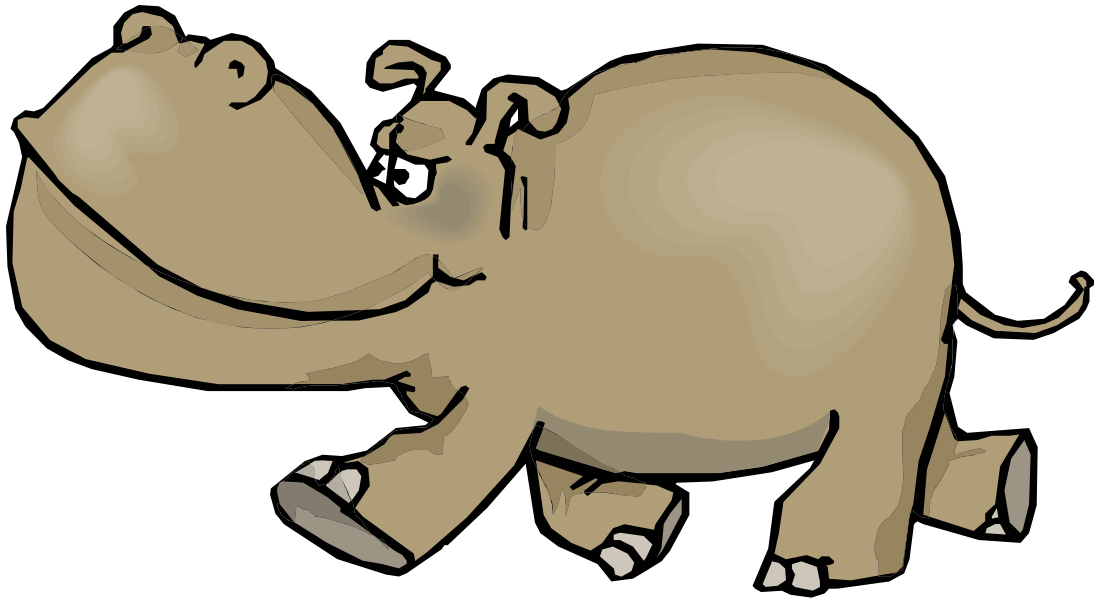
There are seven key elements of an effective healthcare provider corporate compliance program, as recommended by the OIG.

1. Written Policies & Procedures
2. Designation of a Compliance Officer and Compliance Committee
3. Training and Education
4. Effective Lines of Communication
5. Disciplinary Guidelines
6. Auditing and Monitoring
7. Responding to Detected Offenses and Developing Corrective Action Initiatives

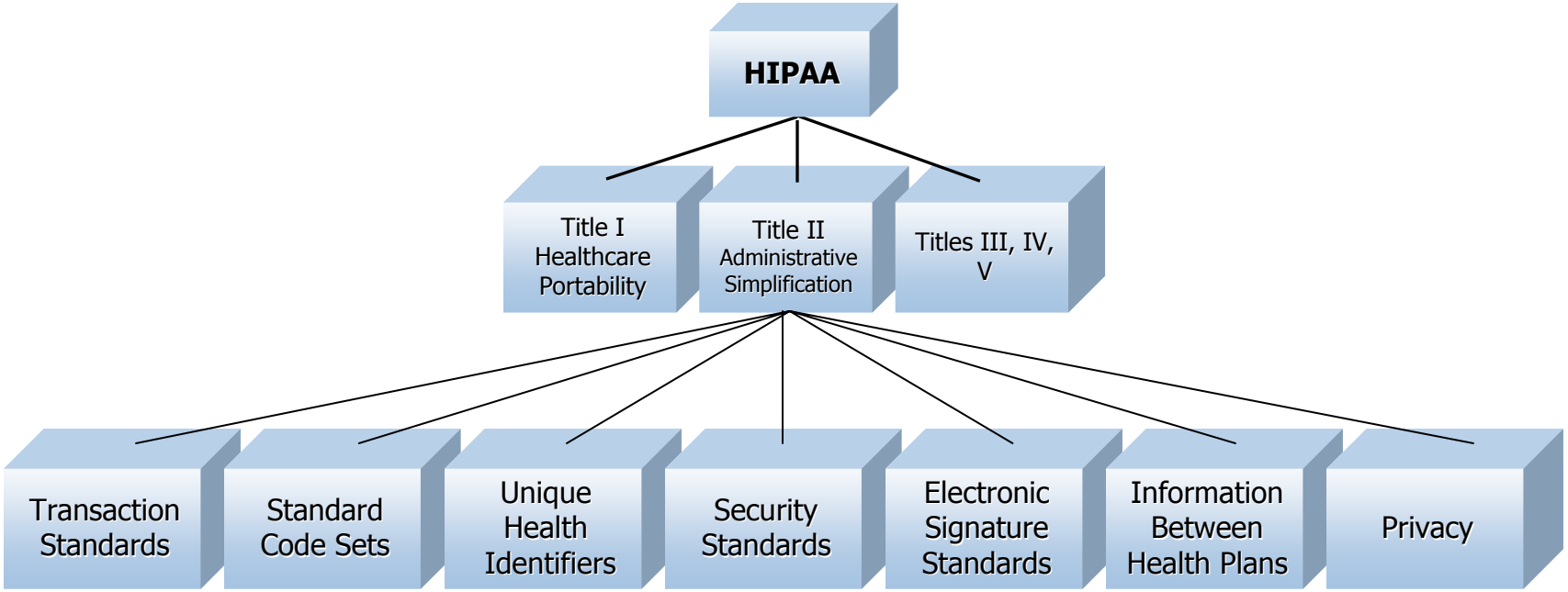
DHHS adhered to these principles when developing the regulatory scheme for HIPAA compliance……

# The HIPAA Compliance Program

**Health Insurance Portability & Accountability Act of 1996 (HIPAA) requires the elements of a Compliance Program that safeguards health information.**

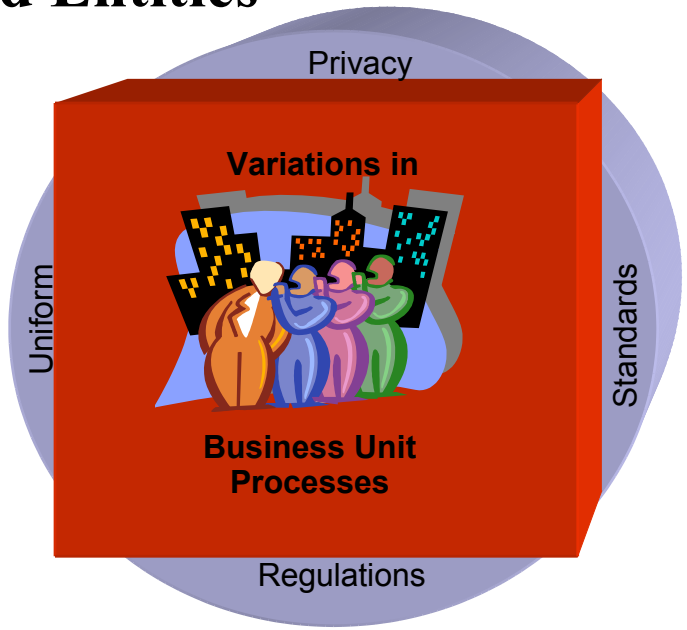


# Health Insurance Portability & Accountability Act of 1996




- Establish standards and requirements for the transmission of certain health information
- Reduce health care fraud and abuse
- Guarantee security of health information
- Require privacy legislation surrounding the use of individually identifiable health information

## Examples of Covered Entities




- Health Care Provider
  - Hospitals
  - Physicians
  - Pharmacies
- Multi-Plan Organization
  - Corporate Parent
  - Separate Health Plans
  - Various State regulations
- Multi-Line Insurance Company
  - Health, Life, Disability, etc.
  - Shared Job Functions
    - Underwriting for both health and other policies
    - Claims adjudication
- HMO Products
  - Combine treatment & payment

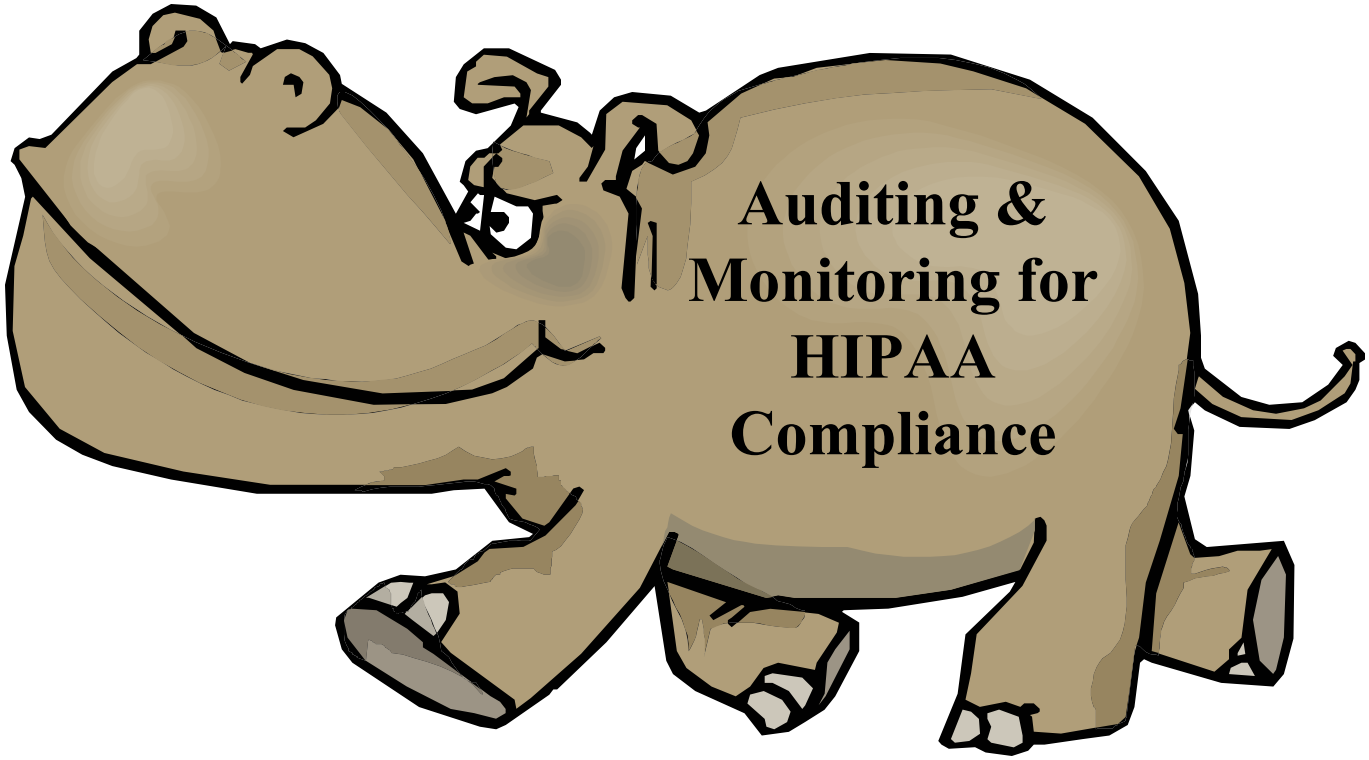
# HIPAA's Current Status and Deadlines

- Transaction and privacy standards are final
  - Additional privacy guidelines finalized 8/14/02
  - Transaction and code set modifications proposed 5/31/02
- Final security standards are expected in ?? 2002
- Employer identifier was finalized on 5/31/02; timeline for other identifiers is uncertain
- Public Law 107-105 provides an extension for standard transactions and code sets until 10/16/03 for covered entities filing an extension request with HHS

| HIPAA Rule | Effective Date | Compliance Deadline |
|---|---|---|
| Privacy | April 2001 & modified August 2002 | April 14, 2003 |
| Transaction Standards | October 2000 | October 16, 2002 ★ |
| Code Sets | October 2000 | October 16, 2002 ★ |
| Unique Identifiers – Employers | July 2002 | July 30, 2004 |
| Unique Identifiers – Individual | On hold | NA |
| Unique Identifiers – Plans, Providers | Proposed | NA |
| Security Standards | April 21, 2003 | April 21, 2005 |

★ EXTENSION REQUESTS FOR 10/16/03

# Auditing & Monitoring



# Integrating HIPAA requirements into the Auditing and Monitoring Process

## Mission & Objectives

- Safeguarding Health Information
- Key Subject Matter Experts
- Compliance Oversight- Privacy Official, Enterprise wide Information Security Structure
- Identify key high risk areas relating to use and disclosure of PHI

## Risk Assessment

- Compliance Issues
- Management Style
- Compliance Structure
- Due Diligence of Compliance with Third Party Agreements

## Audit Plan

- Risk/Control
- Management Focus
- Compliance priorities

## Audit Testing

- Self Analysis
- Best Practices/ Benchmarks
- Controls/Substantive Testing

## Reports & Feedback

- Detail/Summary Reports
- Recommendations
- Performance Assessment
- Special Audits

# Auditing & Monitoring

## HIPAA Compliance Mission and Objectives:

- Safeguarding Protected Health Information ("PHI")
- Identifying risk of improper use and disclosure
- Discussions with Key Subject Matter Experts ("SMEs")
- Review of HIPAA policies and procedures
- Develop foundation for understanding of HIPAA compliance opportunities and risks

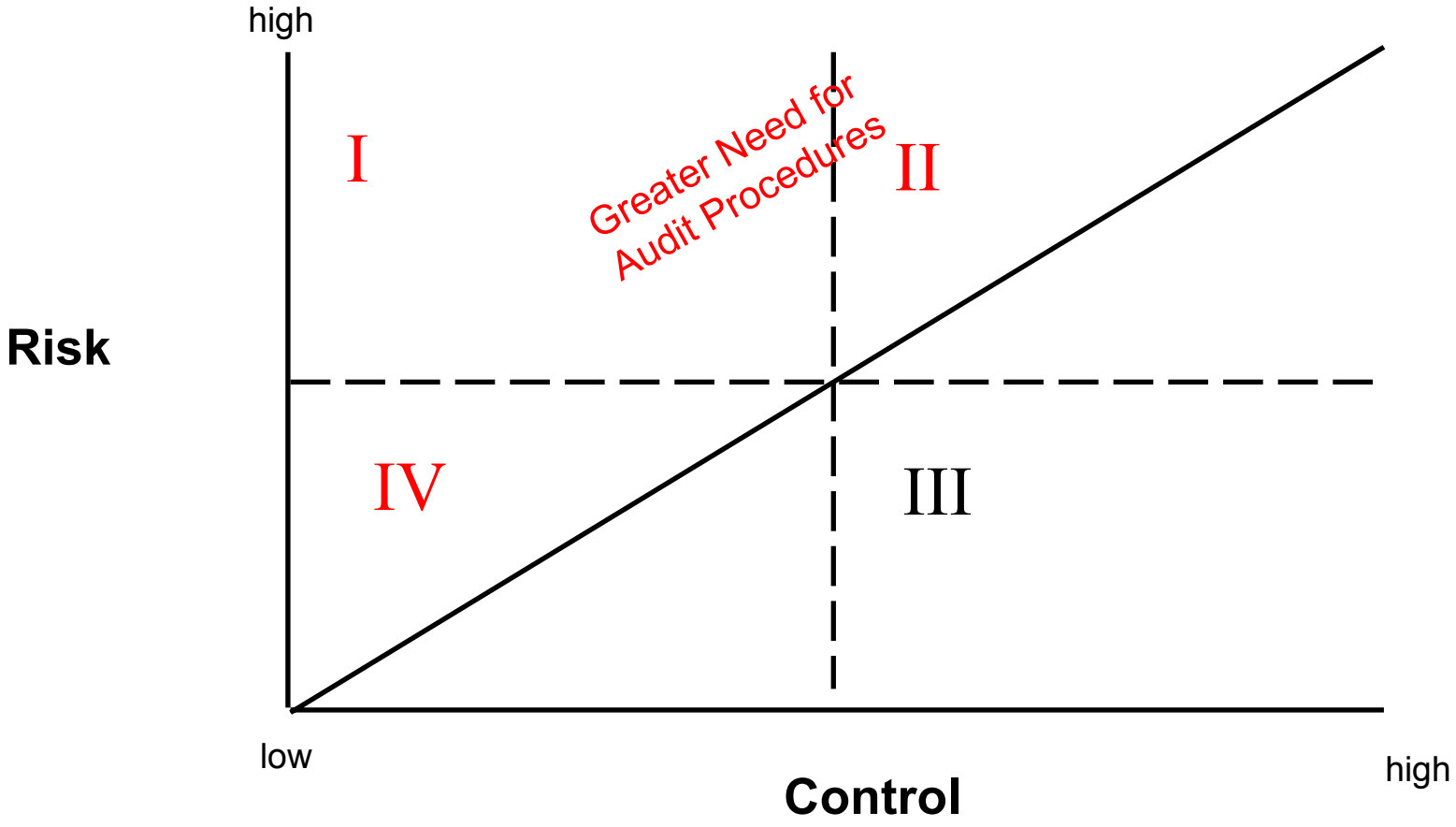
## HIPAA Compliance Risk Assessment

- Used to identify, measure and prioritize compliance risks to help internal auditor evaluate and test critical internal controls
- Requires key SMEs in such departments as Compliance, Human Resources, Claims, Billing, Marketing, Research and other areas that use and disclose PHI
- Provides a dynamic corporate audit plan that identifies proposed audit coverage and "knowledge" resource requirements pertaining to security and privacy requirements
- Internal Auditor recognized as value added business advisor

## HIPAA Compliance Risk Assessment (cont.)

- Evaluate privacy office structure and HIPAA implementation plans to address administrative functions, use and disclosure of PHI, individual rights afforded, and business associate requirements
- An understanding of relationships with third parties such as Business Associates
- Due diligence in response to Business Associates, Chain of Trust and Trading Partners violation of their third party agreements
- Identification of control weaknesses that may cause violations of security and privacy requirements

# Development of Corporate Audit Plan



## HIPAA Compliance Audit Testing

- Audits should focus on areas of vulnerability identified in the initial assessment
- Determine the effectiveness of an institution's HIPAA policies & procedures
  - Work with the HIPAA Privacy Official, Security & TCI SMEs in evaluating and testing the effectiveness of the HIPAA implementation plan policies, procedures and business processes
  - Benchmark by selecting high risk departments and reviewing their policies and procedures to determine if there is a gap between those policies and procedures and HIPAA requirements
-

## HIPAA Compliance Audit Testing (cont.)

- Create ongoing assessment checklists which allow your organization to constantly monitor exposure through use of:
  - HIPAA Implementation Work Plans and DHHS Compliance Guidance Reports
  - Statutes and Regulations distribution
  - Journals and Newsletters distribution

- Implement corporate-wide ongoing self-evaluation process to monitor and validate the effectiveness of the program
  - HIPAA Compliance Department to provide each department with self-monitoring tools to measure against the HIPAA requirements
  - HIPAA Compliance Department can facilitate enforcement of departments' self-evaluation processes

# Auditing & Monitoring

## Reports and Feedback

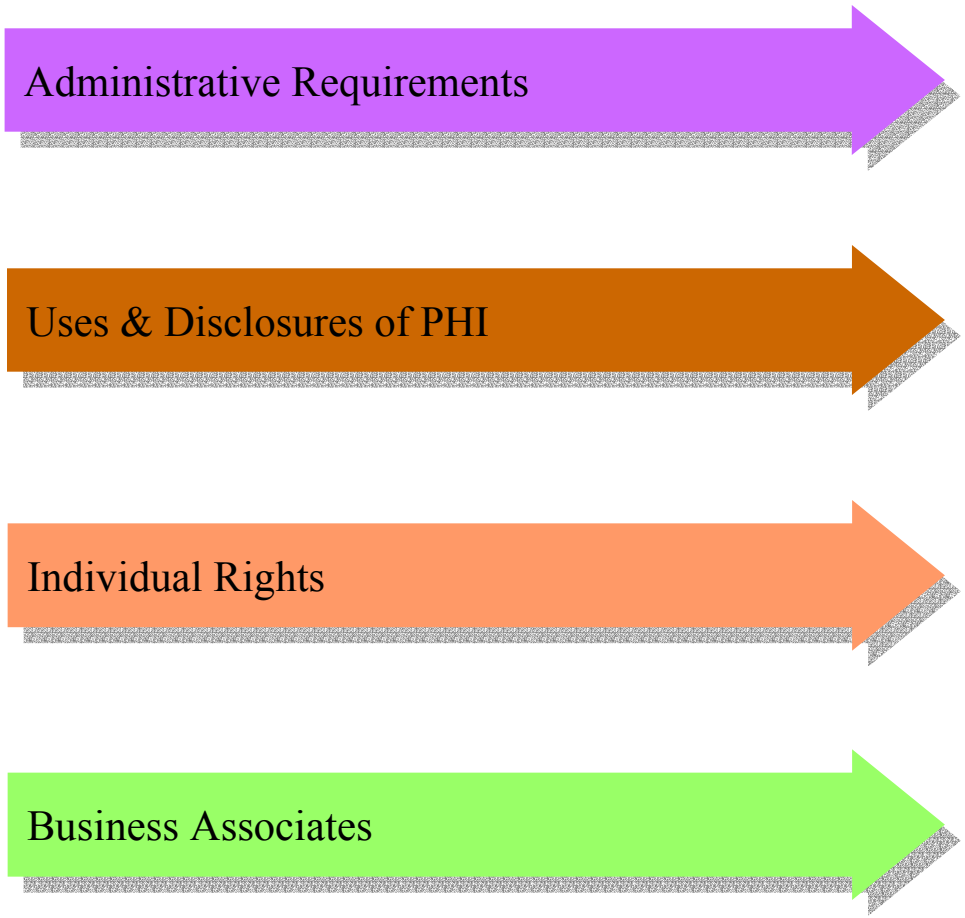
- Recommend corrective measures, including the development of revised policies and procedures, to meet HIPAA requirements
- Significant findings and action taken should be documented and communicated to the Audit Committee, Privacy Office and Committee and Board of Trustees
- Performance assessment of trends identified as control weaknesses and compliance violations
- Reaudit as necessary based upon initial findings and associated risk
- Conduct Special Audits, as needed, i.e. follow up after notification of violation of BA agreement not to disclose PHI

# Auditing & Monitoring – HIPAA Compliance Areas

***It is recommended the following areas be evaluated during an internal HIPAA audit (not inclusive):***

- Accounting
- Actuarial
- Administration
- Agents/Brokers
- Audit
- Billing
- Business Office
- Claims
- Compliance
- Contracts
- Corporate Office
- Enrollment
- Facility Management
- Human Resources
- Information Technology
- Legal
- Marketing
- Medical Staff
- Purchasing
- Records
- Sales
- Treatment
- Underwriting

# Privacy




- Organizational Considerations
- Privacy Official
- Privacy Policies & Procedures
- Employee Education

- Organizational Considerations
- Minimum Necessary
- Authorized Uses & Disclosures
- Special Considerations

- Access to Records
- Request for Restrictions
- Disclosure Accounting
- Amendment of Records

- Identification
- Written Agreement
- Non-compliance Process
- Due Diligence

# Auditing & Monitoring - Privacy

Administrative:

- Determine if a Privacy Official has been appointed.
- Determine that employees have been trained on the organization's privacy policies and general HIPAA requirements.
- Review procedures relating to disclosing or transmitting member information.
- Determine if there is a process to monitor HIPAA compliance.
- Determine if there is a process in place to address individual complaints about privacy violations.
- Determine if there is a process in place for the organization to take corrective action for violations.
- Determine if there is a policy in place to address employee discipline and a process to accomplish this for privacy violations.

# Auditing & Monitoring - Privacy

## Use and Disclosure of PHI:

- Evaluate if there are procedures or processes in place to check that if an individual has given the organization written permission to make a disclosure, if necessary.
- Determine if a process is in place to identify appropriate uses of PHI.
- Determine if a process is in place that identifies routine and non-routine disclosures of PHI.
- Determine if a minimum necessary policy is in place for the organization to respond to requests for and disclosures of PHI.
- Determine if a verification process is in place.
- Determine if any policies and procedures exist with respect to the organization's group health plan and if so, whether there are any processes in place that restrict the disclosure of employee health information and address the plan document.

# Auditing & Monitoring - Privacy

## Use and Disclosure of PHI (cont.):

- Determine if the organization has a system to track disclosures as required.
- Determine if a policy exists to determine if authorizations are valid.
- Determine if a policy or process is in place to require minimum necessary use and disclosure, noting exceptions (e.g., physician requests, individual requests).
- Determine if there is a process in place to designate the record set for an individual.
- Determine if departments have a policy that addresses deleting all PHI from member information before disclosing the information outside the company.
- Determine if there is a process in place to obtain patient authorization for marketing and fundraising activities.

# Auditing & Monitoring - Privacy

## Individual Rights:

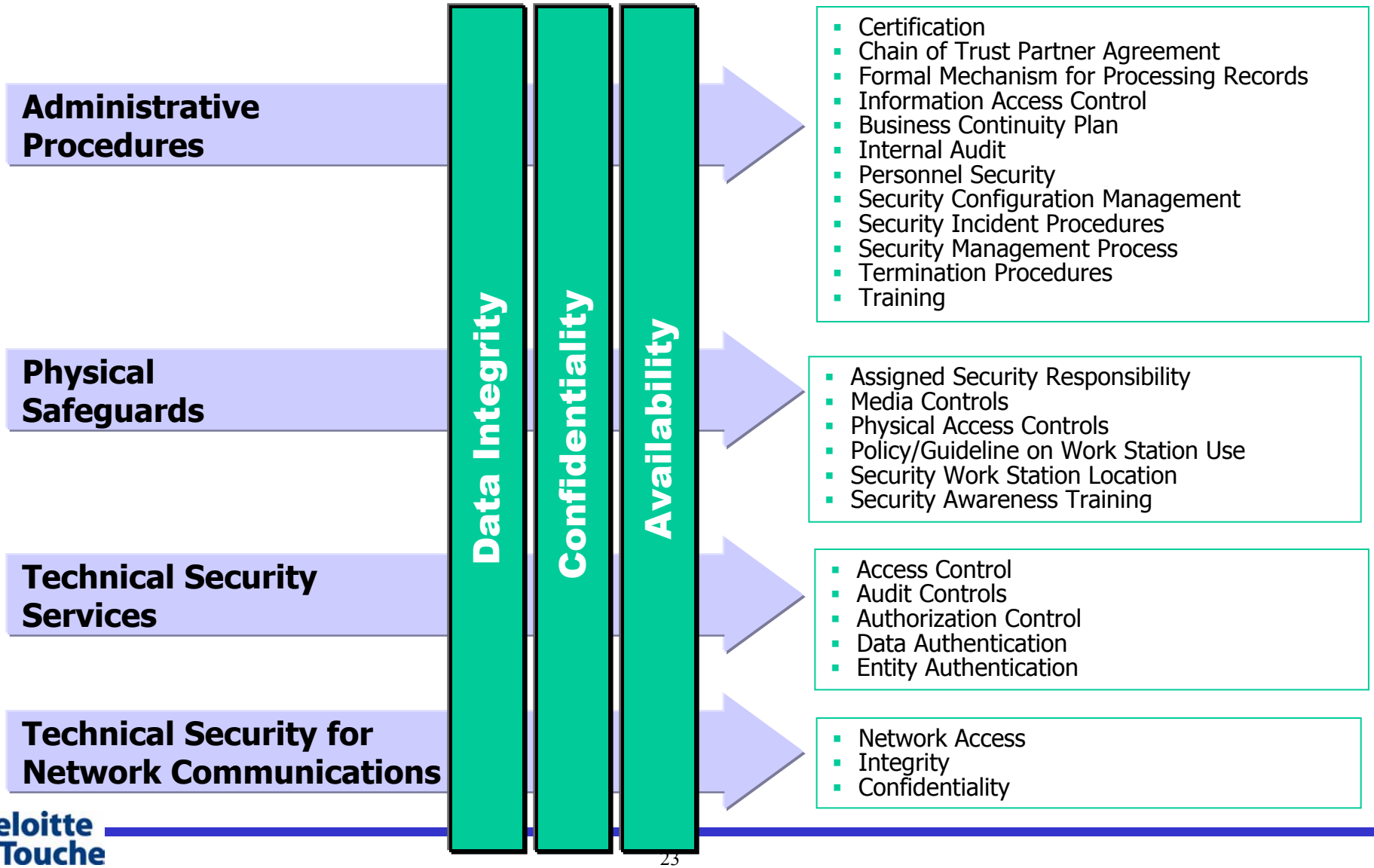
- Determine if there is a process in place that requires the organization to permit individuals the right to access, copy and amend their protected health information.
- Determine if there is a process in place that requires the organization to respond to requests for restrictions on disclosure.
- Determine if there is a policy in place that addresses accounting for individual PHI disclosure.
- Determine if there is a policy in place to address individuals' requests not to be in a facility directory.

# Auditing & Monitoring - Privacy

Business Associates:

- Determine if there is a process in place to address Business Associate Agreements.
- Determine if there is a process in place to identify and maintain current lists of Business Associates.
- Determine if there is a policy in place to address non-compliance with Business Associate Agreements.

# Security


Administrative Procedures
Physical Safeguards
Technical Security Services
Technical Security for Network Communications
Data Integrity
Confidentiality
Availability
Certification
Chain of Trust Partner Agreement
Formal Mechanism for Processing Records
Information Access Control
Business Continuity Plan
Internal Audit
Personnel Security
Security Configuration Management
Security Incident Procedures
Security Management Process
Termination Procedures
Training
Assigned Security Responsibility
Media Controls
Physical Access Controls
Policy/Guideline on Work Station Use
Security Work Station Location
Security Awareness Training
Access Control
Audit Controls
Authorization Control
Data Authentication
Entity Authentication
Network Access
Integrity
Confidentiality

# Auditing & Monitoring - Security

- Administrative Procedures - Evaluate documented administrative procedures pertaining to the selection and execution of security measures that protect data and manage the conduct of personnel in relation to the protection of data.
- Physical Safeguards - Evaluate the physical computer systems and related buildings and equipment for protection from fire and other natural environmental hazards, including intrusion.
- Technical security services - Evaluate the processes in place that protect information and control individual access to information.
- Technical security mechanisms - Evaluate the processes in place that guard against unauthorized access to data that is transmitted over a communications network.
- Electronic signatures - Evaluate if there are electronic signatures, and if in place, determine if they are used on electronic documents to bind it to a particular entity.

# Auditing & Monitoring - TCI

## Monitoring Activities During HIPAA Implementation:

Measure implementation progress against detailed HIPAA readiness workplans:

- Check implementation progress against established deadlines.
- Review electronic testing plans and results of tests.
- Run code scans to determine whether prohibited codes have been eliminated.

# Auditing & Monitoring - TCI

## Ongoing Monitoring Activities:

- Determine if there are edit mechanisms in place to flag noncompliant transactions. Test system edits.
- Perform ongoing testing of transactions to confirm that the HIPAA transaction requirements (e.g., new transactions, addenda to existing transactions) are implemented.
- Perform coding reviews on a periodic basis. Compare an electronic file of HIPAA compliant codes to an electronic file of codes used and test for discrepancies. Alternatively, review log books for new code requests.
- Review the budget to determine if it needs to be updated for additional remediation.

**Sheryl Vacca, Director**

**Deloitte & Touche, LLP**

**svacca@deloitte.com**

**714-436-7710 or**

**916-498-7156**

**Suzie Draper**

**Intermountain Health Care**

**Corporate Compliance Administrator**

**801-442-6516**

# Questions and Answers