

# Second National HIPAA Summit

## Integrating Privacy and Security Implementation Features

M. Peter Adler, JD, LLM

Robyn A. Meinhardt, RN, JD

March 2, 2001

# Agenda

- ◆ Overlap Between Security and Privacy
- ◆ Reaching Efficiencies in the Assessment and Implementation Process

# Overlap Between Security and Privacy

# Common Regulatory Terms

- ◆ §164.530. Safeguards. A covered entity must have in place appropriate *administrative, technical, and physical* safeguards to protect the privacy of protected health information.
- ◆ §142.308 of the Proposed Security Standard requires *administrative, technical and physical* measures to guard the data integrity, availability and confidentiality

# Privacy and Security Overlap



# Coordinating Privacy and Security Implementation

- ◆ Security: Personnel security (maintaining records of access authorizations; granting and verifying proper access authorizations; personnel clearance procedure)
- ◆ Privacy: Link to -
  - ◆ All use/disclosure policies
  - ◆ Minimum necessary access policy and
  - ◆ Sanction policy

# Coordinating Privacy and Security Implementation

- ◆ Security: Internal audit of system activity (log-ins, file access, security incidents)
- ◆ Privacy: Link with all access/use/disclosure policies and with sanction policy
- ◆ Privacy: Link with “accounting to patients for disclosures” policy
- ◆ Other: Link to other legal audit policies

# Coordinating Privacy and Security Implementation

- ◆ Security: Security configuration management procedures and responsibility
- ◆ Privacy: Link to “changes to information practices” policy (some changes may affect technology configuration)
- ◆ Privacy: Coordinate with IT contracting, legal (for licensing, software compliance)

# Coordinating Privacy and Security Implementation

- ◆ Security: Security Incident Procedures
- ◆ Privacy: Link to “accounting to patients for disclosures” and “mitigation” policies;
- ◆ Coordinate with sanction policy

# Coordinating Privacy and Security Implementation

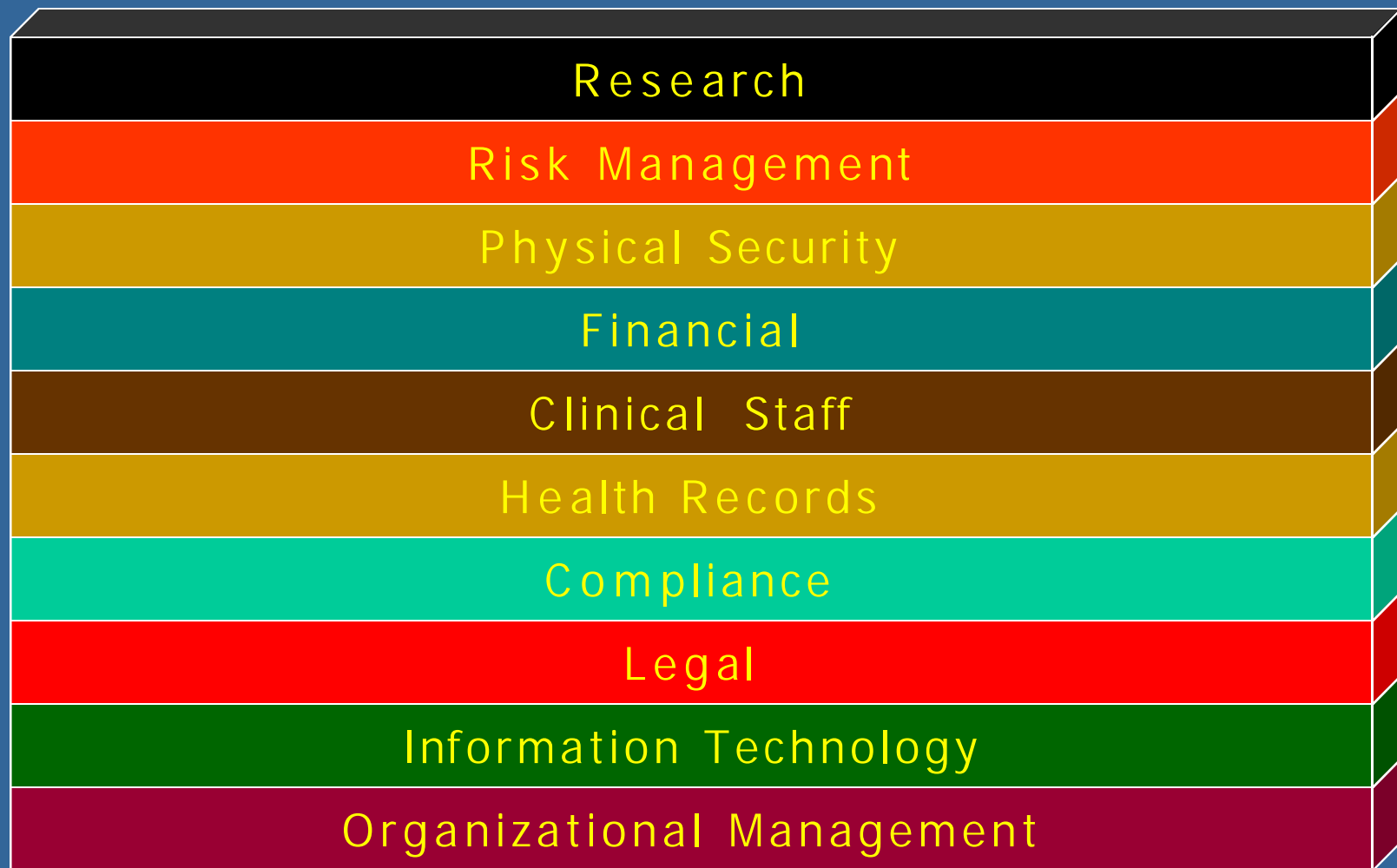
- ◆ Security: Personnel termination procedures; procedures for verifying authorized access
- ◆ Privacy: No longer members of the work force
- ◆ Minimum necessary access policies
- ◆ Sanction policies

# Coordinating Privacy and Security Implementation

- ◆ Security: Security Officer job description
- ◆ Privacy: Coordinate with Privacy Officer job description; provide for collaboration

**Departments must collaborate...**

# Security/Privacy Officers: Interdepartmental Coordination



# Coordinating Privacy and Security Implementation

- ◆ Security: Media controls, information access controls (including access authorization, establishment, and modification)
- ◆ Privacy: Coordinate with “minimum necessary” policy; authorized access/use/disclosure policies; de-identification policy; accounting for disclosures policy

# Coordinating Privacy and Security Implementation

- ◆ Security: Training in security awareness
- ◆ Privacy: Training in privacy policies and requirements

**Combine security and privacy training**

# Coordinating Privacy and Security Implementation

- ◆ Security: No specific compliance section or document retention requirements, but written policies and procedures are required
- ◆ Privacy Compliance: Policy documentation, revision and retention requirements

**Check for compliance and retention requirements in final security regulations**

# Coordinating Privacy and Security Implementation

- ◆ Security/IT: (technical expertise re: removal of data elements, and in certifying de-identification of data)
- ◆ Use technical means to protect data before de-identification
- ◆ Privacy: De-identification of data policy; certification of de-identification

# Coordinating Privacy and Security Implementation

- ◆ Security: (link from security sanctions policy to this privacy policy)
- ◆ Privacy: Policy on refraining from retaliatory or intimidating acts

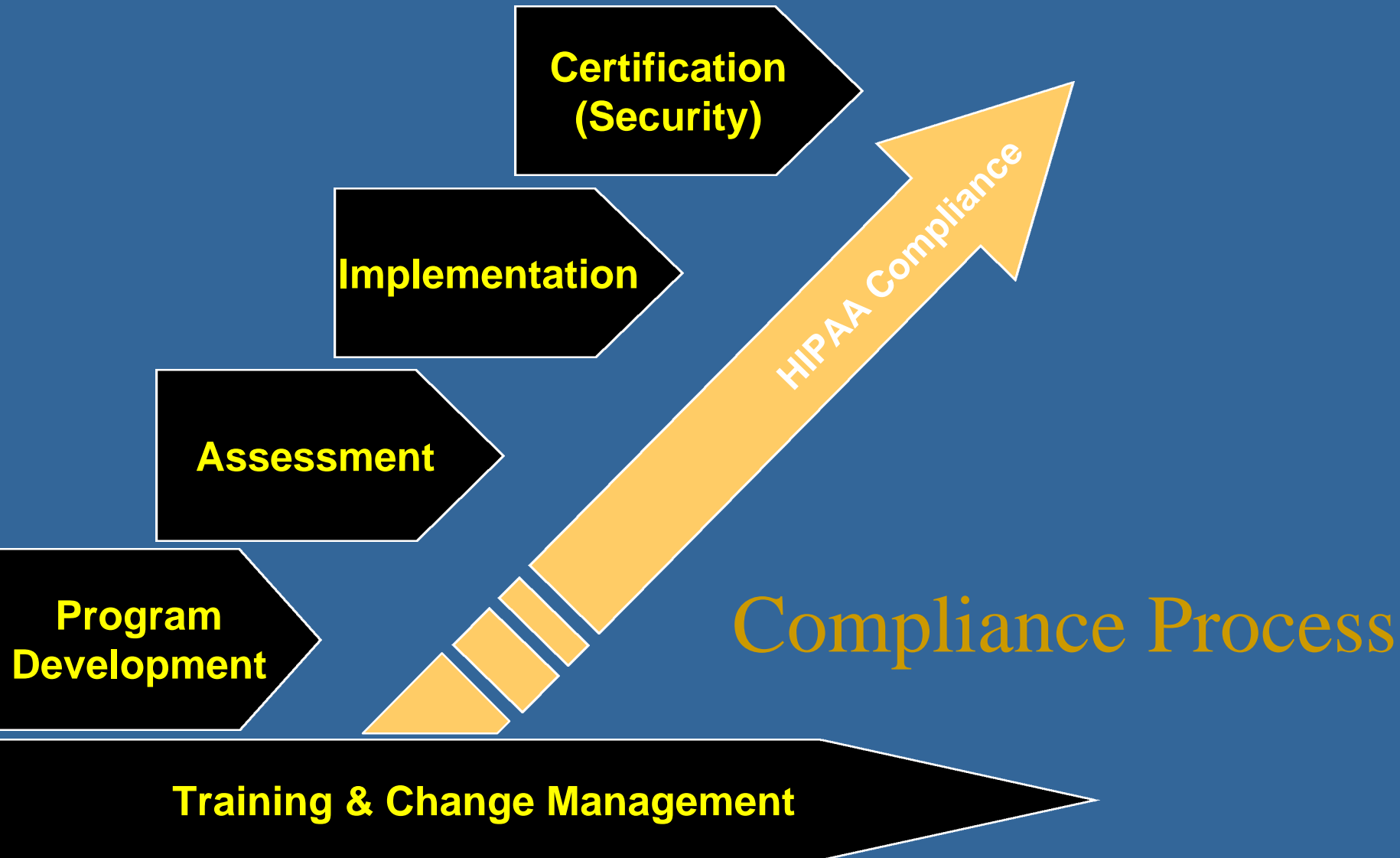
# Coordinating Privacy and Security Implementation

- ◆ Security: Requirement for formal mechanisms for processing records (routine and non-routine receipt, manipulation, storage, dissemination, transmission and /or disposal of health information)
- ◆ Privacy: coordinate with (or make the same as) all access/use/disclosure policies; “minimum necessary” policy; designated record set determinations; and accounting for disclosures policy

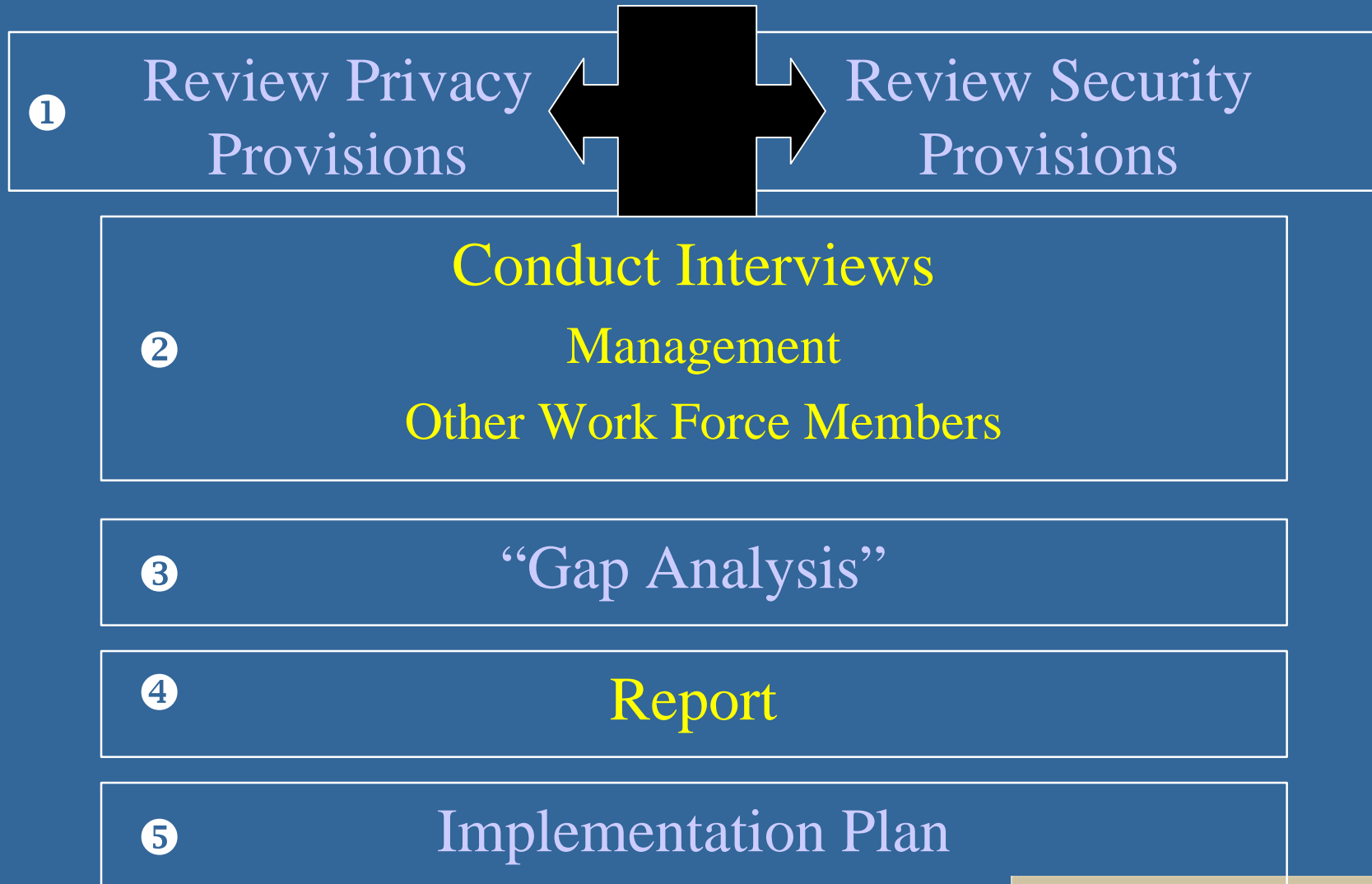
# HIPAA Contracts

- ◆ Chain of Trust
  - ◆ Derivative security obligations
- ◆ Business Associate
  - ◆ Carry out transaction functions on behalf of a covered entity and deemed to act for the entity
  - ◆ Derivative confidentiality obligations
- ◆ Trading Partner Agreement
  - ◆ Terms of the EDI transactions

# Reaching Efficiencies in the Assessment and Implementation Process



# Achieving Efficiencies in Policies and Procedure Review



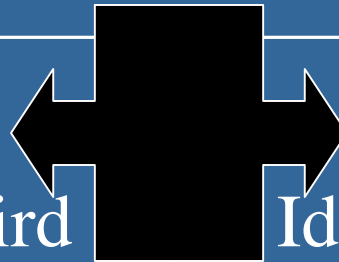
# Achieving Efficiencies in Contract Review

Vendors, Physicians Clinical laboratories, Pharmaceutical companies (research sponsors), Health Plans, Employers, Other Business Associates

①

Technical Team

Identification of Third Parties on System

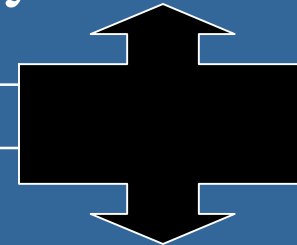


Legal Team

Identification of Third Parties  
Interviews, Contracts

②

Security Contract Issues



Privacy Contract Issues

# Questions

Robyn A. Meinhardt  
Foley & Lardner  
1999 Broadway, Suite 2560  
Denver, CO 80202  
303-294-4414  
rmeinhardt@foleylaw.com

M. Peter Adler  
Foley & Lardner  
3000 K Street NW  
Washington, DC 20007  
202-945-6146  
padler@foleylaw.com