# Incorporating Privacy Policies and HIPAA Compliance into an Institutional Compliance Plan

**Rebecca L. Williams, RN, JD**
**Davis Wright Tremaine LLP**
**1501 Fourth Ave.**
**Seattle, Washington**
**(206) 628-7769**
**beckywilliams@dwt.com**

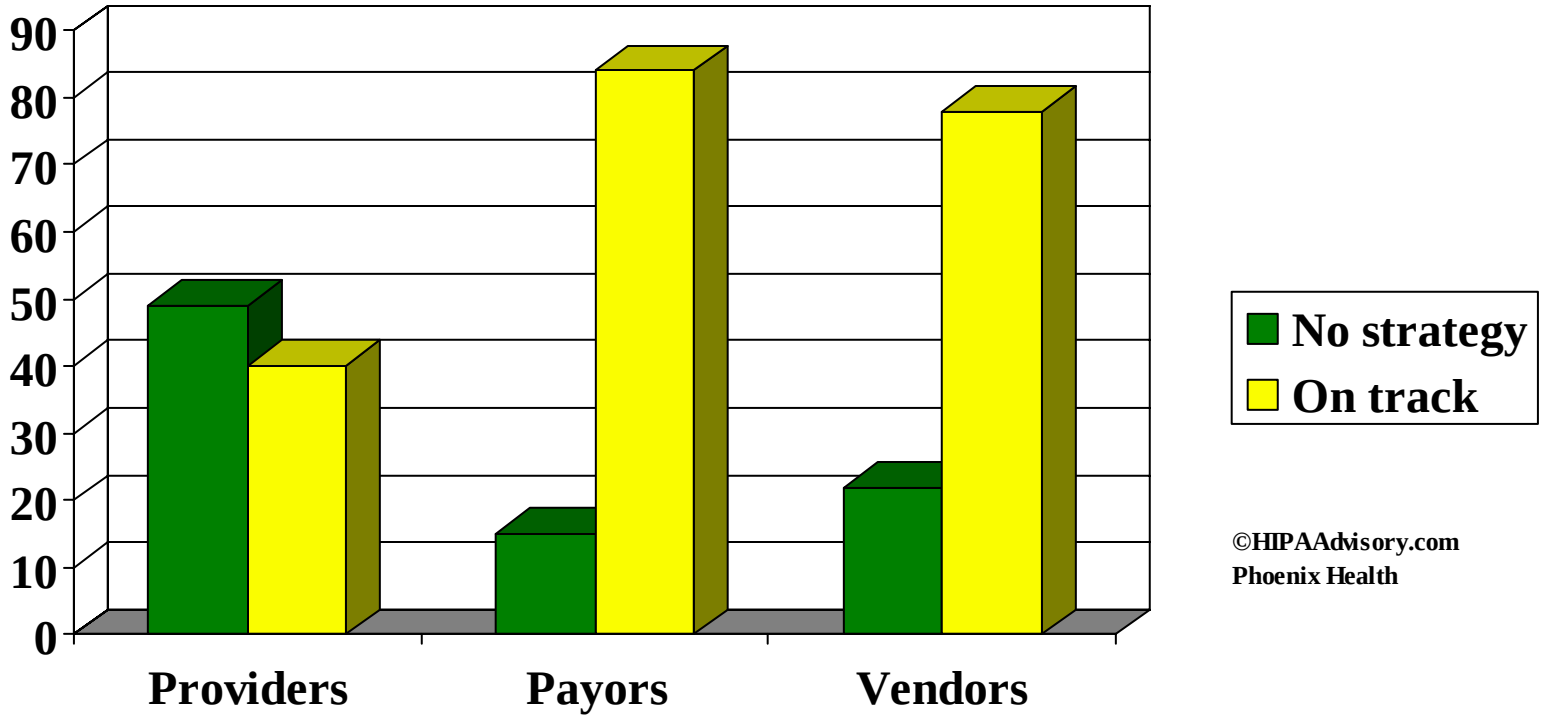
**Shana Chung, MPH, JD**
**Premera Blue Cross**
**PO Box 327**
**Seattle, WA 98111**
**(425) 670-4356**
**shana.chung@premera.com**

**Davis Wright Tremaine LLP**

# The HIPAA Clock Is Ticking

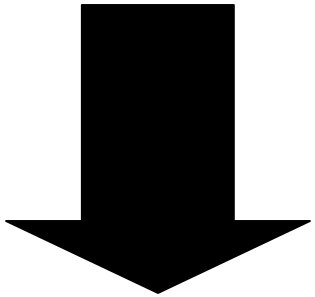
- The final transaction and code sets regulations started the clock
- Standards must be implemented by October 16, 2002 (with an extra year for small health plans)
- The other regulations are not far behind

# HIPAA Compliance Strategy Progression



# Commitment to HIPAA Compliance

- HIPAA compliance needs to be top-down
- Start with an education process, including the board and senior leadership
- Must have commitment to compliance by the board and senior leadership



# Practical Reasons for Compliance Plans

- **Reduce criminal and civil liability/based on the Federal Sentencing Guidelines**
- **Government encouragement — Compliance Program Guidance**
- **Consistent with Board's fiduciary duty**
- **Consistent with sound business practices**
- **Voluntary is preferable over government-mandated plan**

# A First Step — Revisit Corporate Compliance Programs

- Organizational commitment to integrity
- Form of self-policing
- Processes to effectively ensure legal compliance
- Part of an organization's day-to-day operations
- Part of the health care industry

# Integrated Compliance Planning

- For those with compliance programs, leverage current compliance knowledge, processes, culture and resources
- For those without effective compliance plans
  - Use HIPAA as the lead issue
  - Establish structure — Expand as capabilities allow
- Integrate — Do not just layer an additional bureaucracy on top

# Integrated Compliance Planning

| *OIG Compliance Plan* | *HIPAA Compliance Plan* |
|---|---|
| Policies & Procedures | Administrative Procedures |
| Assignment of Oversight Responsibilities | Assigned Security & Privacy Responsibilities |
| Training & Education | Training & Education |
| Lines of Communication | Report Procedures; Event Reporting |
| Enforcement & Discipline | Sanctions |
| Audit & Monitoring | Internal Audit |
| Response & Corrective Action | Response Procedures; Testing & Revision |

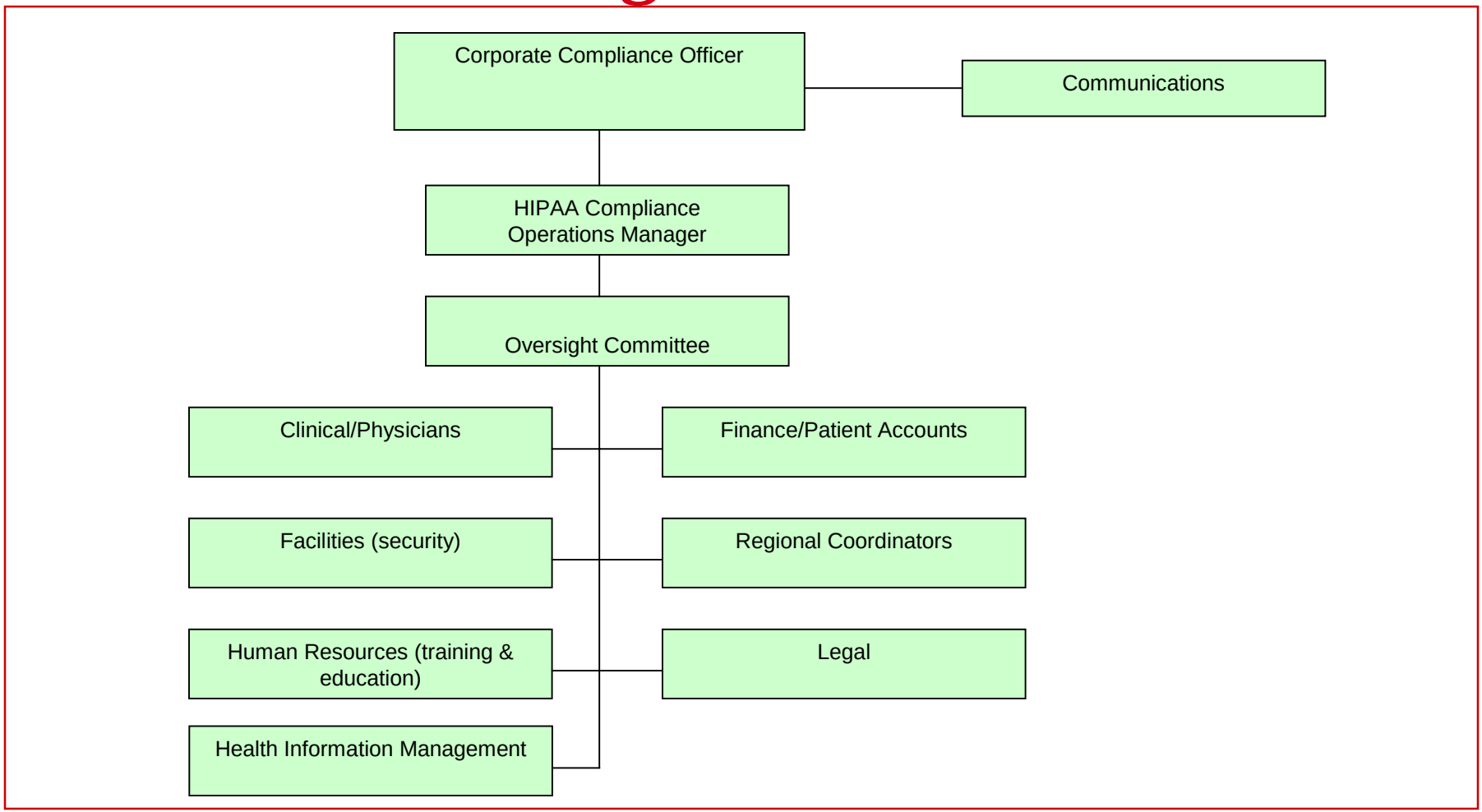
# Ensure Oversight — Compliance Task Force

- Form HIPAA oversight group or task force
- Too big a job for one person
- Engage key managers and clinicians
- Don't delegate this solely to the I/S department

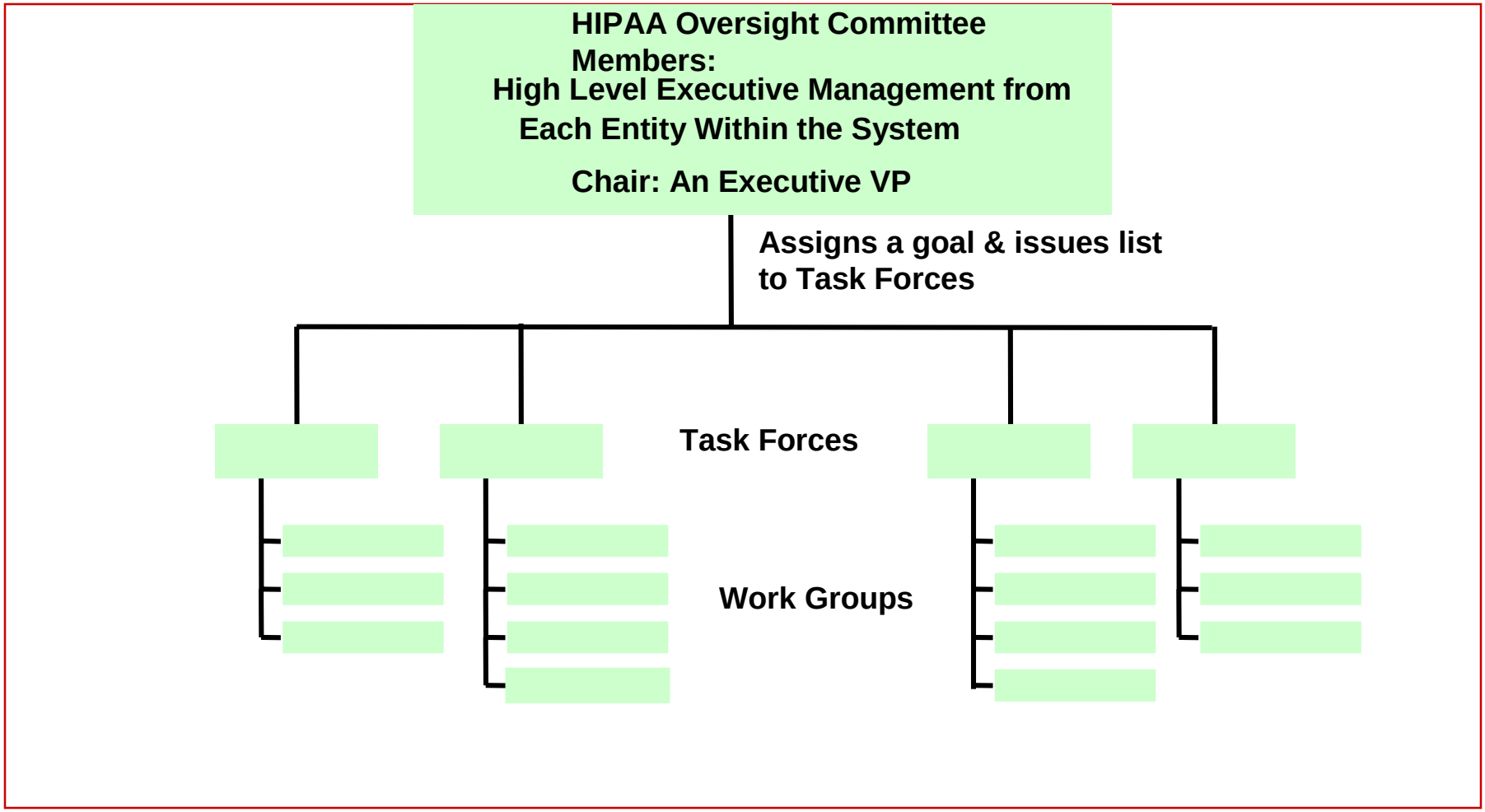
# Ensure Oversight — HIPAA Police

- Appoint privacy and security officials
- Must have real authority — Be aware of the chain of command
- Defined by organization's need
- Who should be privacy and security officer?

# Ensure Oversight — Other HIPAA Organizational Structure



# Ensure Oversight — Other Structures



# Employee Training: Like All Compliance Efforts, Training Is Crucial

- Privacy and security awareness training to —
  - Entire workforce
  - New employees
- When policies change, retrain affected employees
- HIPAA certification for employees
  - New certification statement at least every 3 years
  - May want to tie with compliance program
- Stress importance of security and privacy
- Consistent enforcement

# Risk Management

- Prioritize the issues facing the organization
- Priorities list should drive the compliance plan
- Fix identified problems in priority order

# HIPAA Project Scope

- Compliance for all Premera entities impacted by HIPAA
- Modification of information systems
- Modification of business practices
- Document policies and procedures
- Draft business partner agreements
- Secure transmission & storage of all protected health information
- HIPAA compliance monitoring

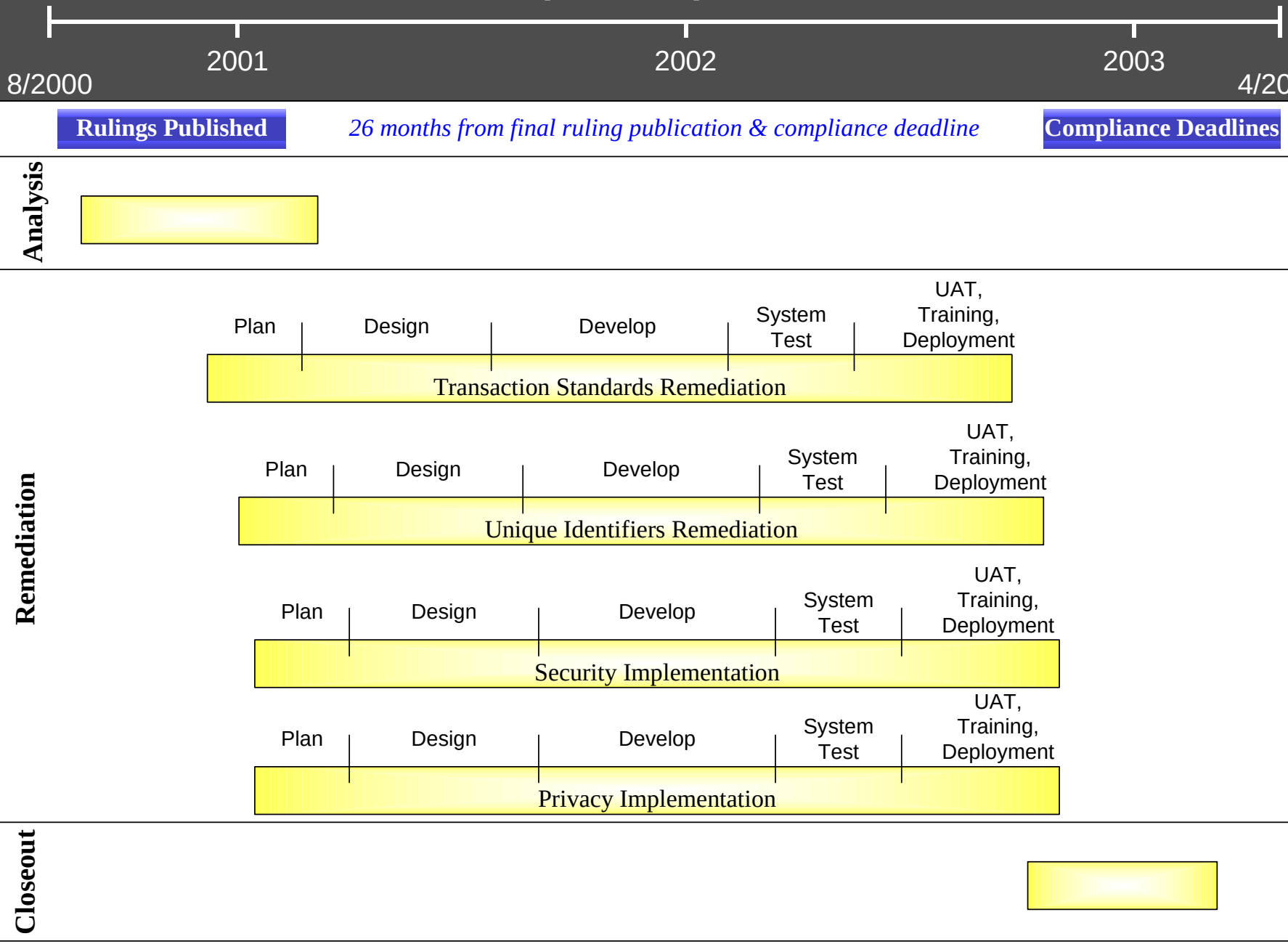
# HIPAA Program Phases

*Decide on Remediation Strategy*

| Phase | Assessment | Analysis | Remediation | Closeout |
|---|---|---|---|---|
| Content | ✓ High Level Assessment<br>✓ Identify impacted systems and processes<br>✓ High Level Scope<br>✓ Total Project Cost Gross Estimate | ✓ Select HIPAA Consultant<br>❑ Detailed Gap Analysis of affected systems and processes<br>❑ Code Analysis<br>❑ Transaction Gap Analysis<br>❑ Operational Gap Analysis<br>❑ Data Dictionary & Data Mapping<br>❑ Security Design<br>❑ Privacy Analysis<br>❑ Remediation Approach Decision<br>❑ Remediation Plan and Schedule | ❒ Detailed system design of remediation<br>❒ Detailed design of procedural changes<br>❒ Coding and testing<br>❒ Implementation of system remediation and procedural changes<br>❒ Communication and retraining<br>❒ Trading Partner contract modifications<br>❒ Finalize contracts with vendors & contractors | ❒ Transition project team |
| Timing | Jan 00 – Mar 00 | Sep 00 – Mar 01 | Nov 00 – Mar 03<br>Staggered stages which begin as each ruling is published | Apr 03<br>Follows each remediation stage |

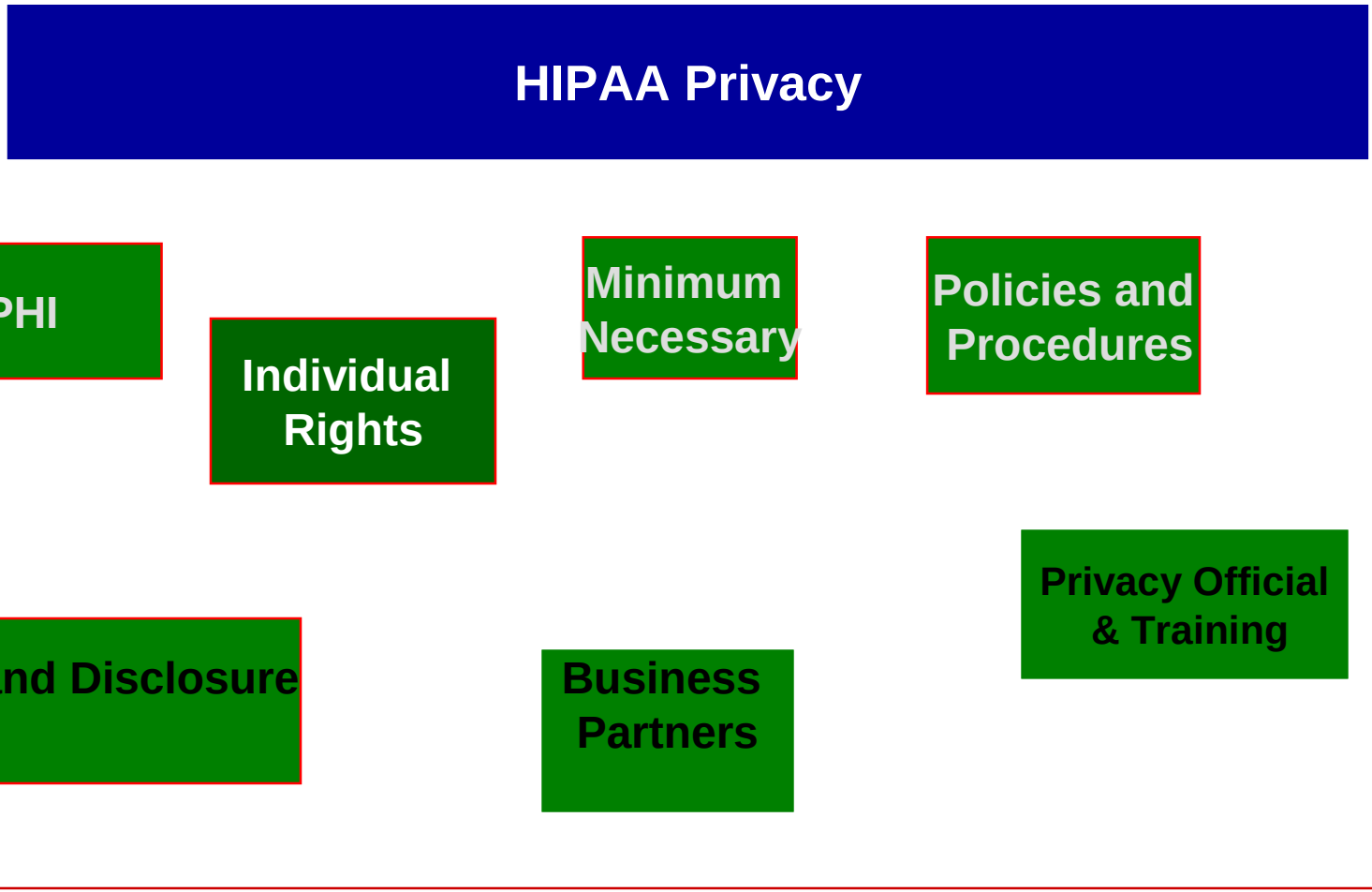
# *HIPAA Program Schedule*

***September 2000 - April 2003***

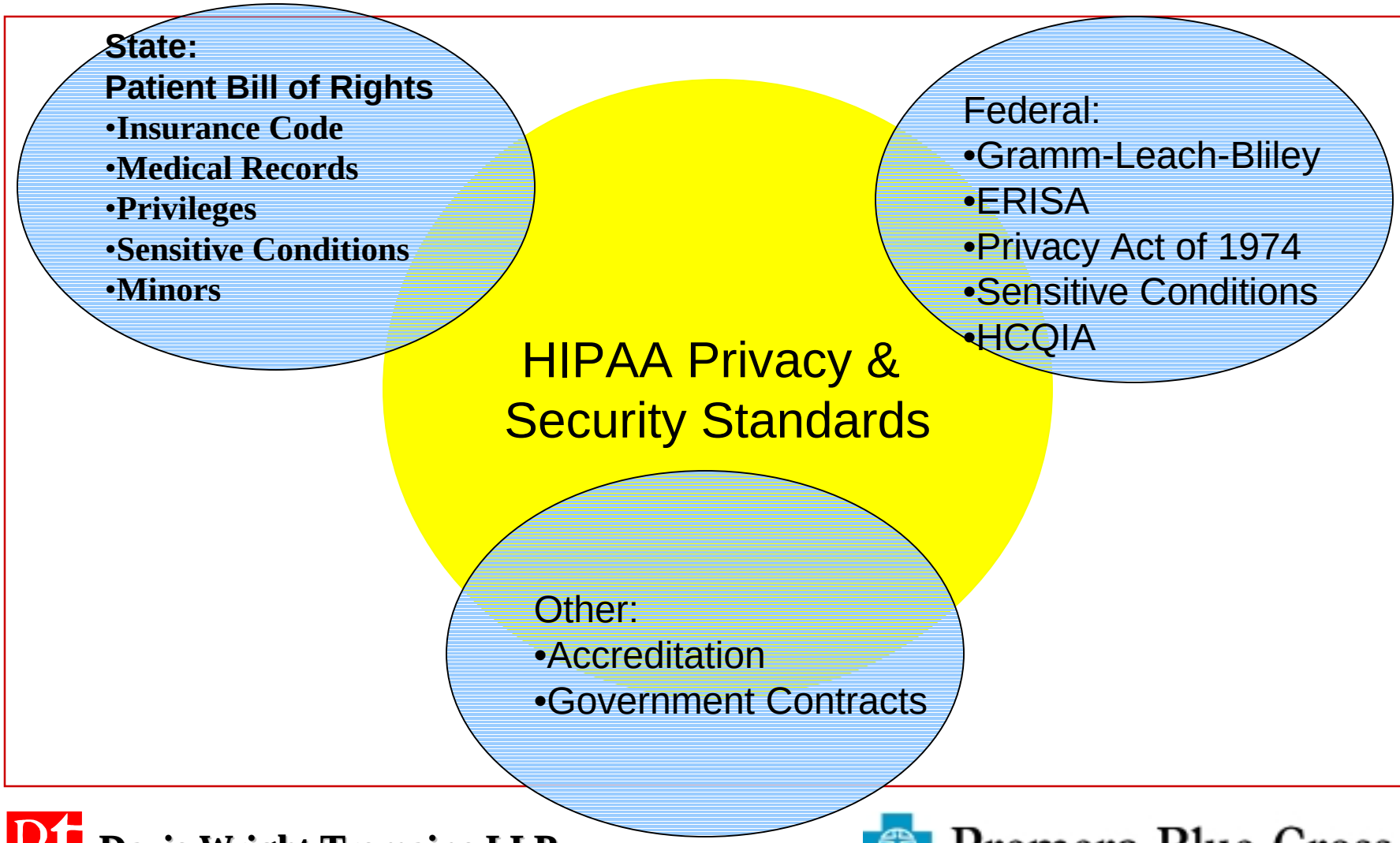


# Know the HIPAA Rules

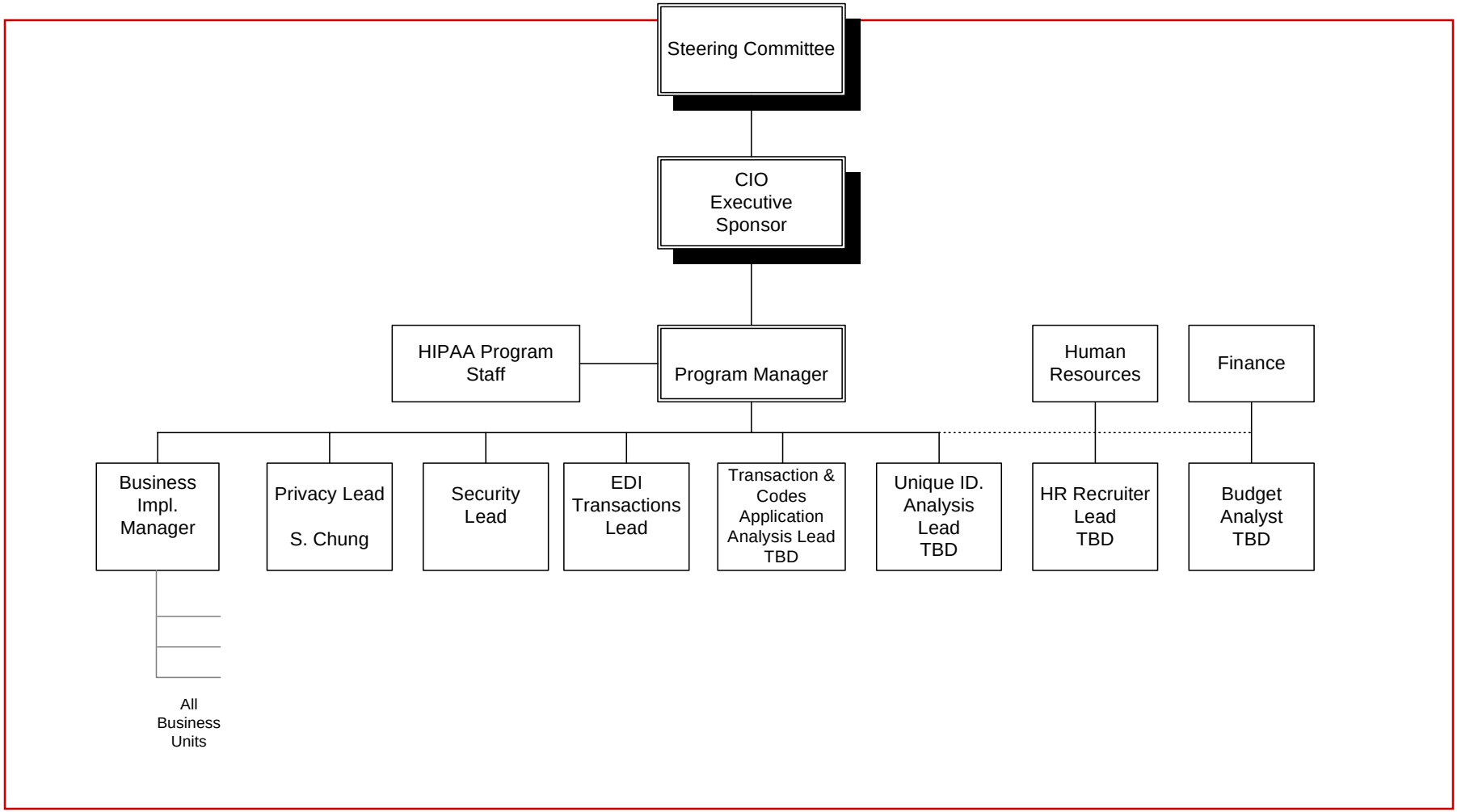
Overview



# Know Related Rules



# Build the HIPAA Team



# Analysis Phase Staffing

**Program Core Team**

- Program Manager
- Business Implementation Manager
- 3 Project Managers
- Standard Transactions Lead
- Application Analysis Lead
- Unique Identifier Lead
- Security Lead
- Privacy Lead

**PMO Staff**

- Project Coordinator
- Project Financial Analyst
- Project Administrator/Technical Writer/Webmaster
- HR Recruiter
- Information Modeler
- Data Analyst
- Architect
- Business Analyst

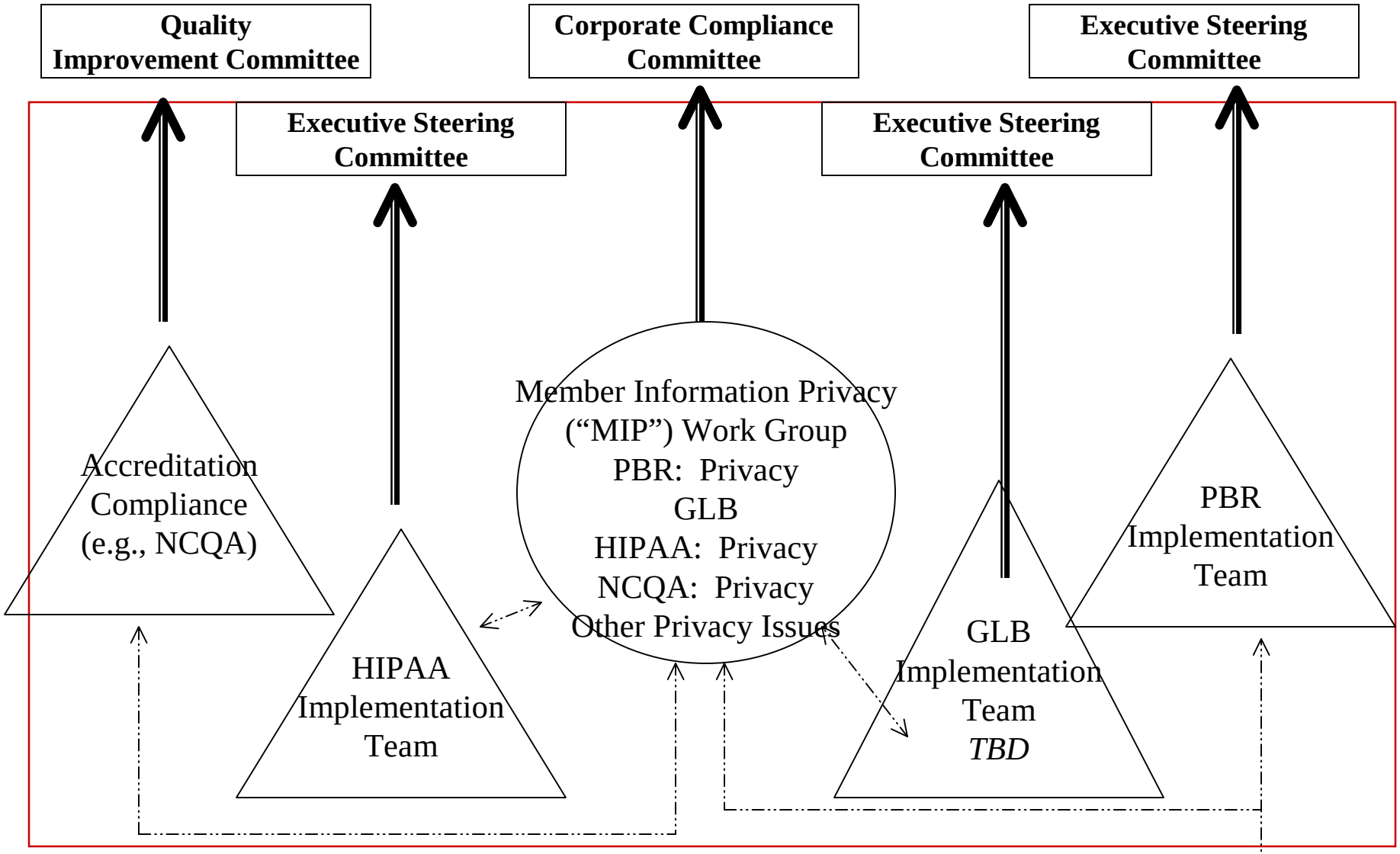
**Subject Matter Experts**

- 100 Business Experts x 16 hr (avg)
- 80 System Experts x 16 hr (avg)

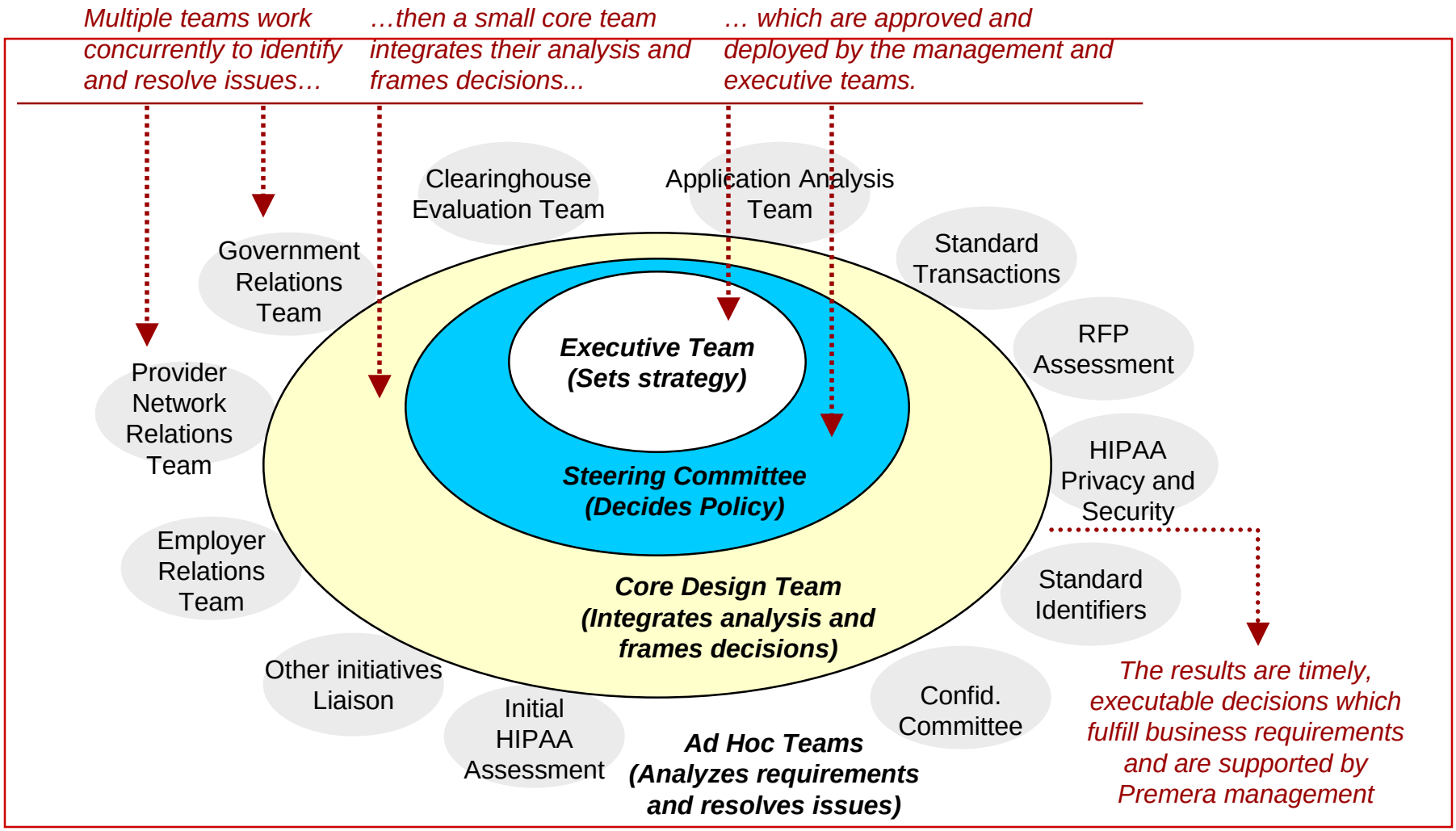
# Conduct Assessment and Analysis

- Inventory Data Repositories
  - Identify where information resides
  - Look beyond the obvious (palm pilots, laptops)
- Evaluate current processes
  - Technical
  - Human
  - Organizational
- Y2K inventories may be helpful
- DON'T STOP with information systems!

## Reporting Structure: Privacy Issues



# Ad Hoc Analysis & Implementation Teams



# Final Thoughts

- The HIPAA clock is ticking
- Start now and keep at it
- Integrate HIPAA into your strategic vision
- Comprehensive organizational plan
- If you base HIPAA compliance decisions on sound business practices and the best interest of individuals, you probably will meet or exceed HIPAA's requirements