

# **HIPAA Assessments and Next Steps**

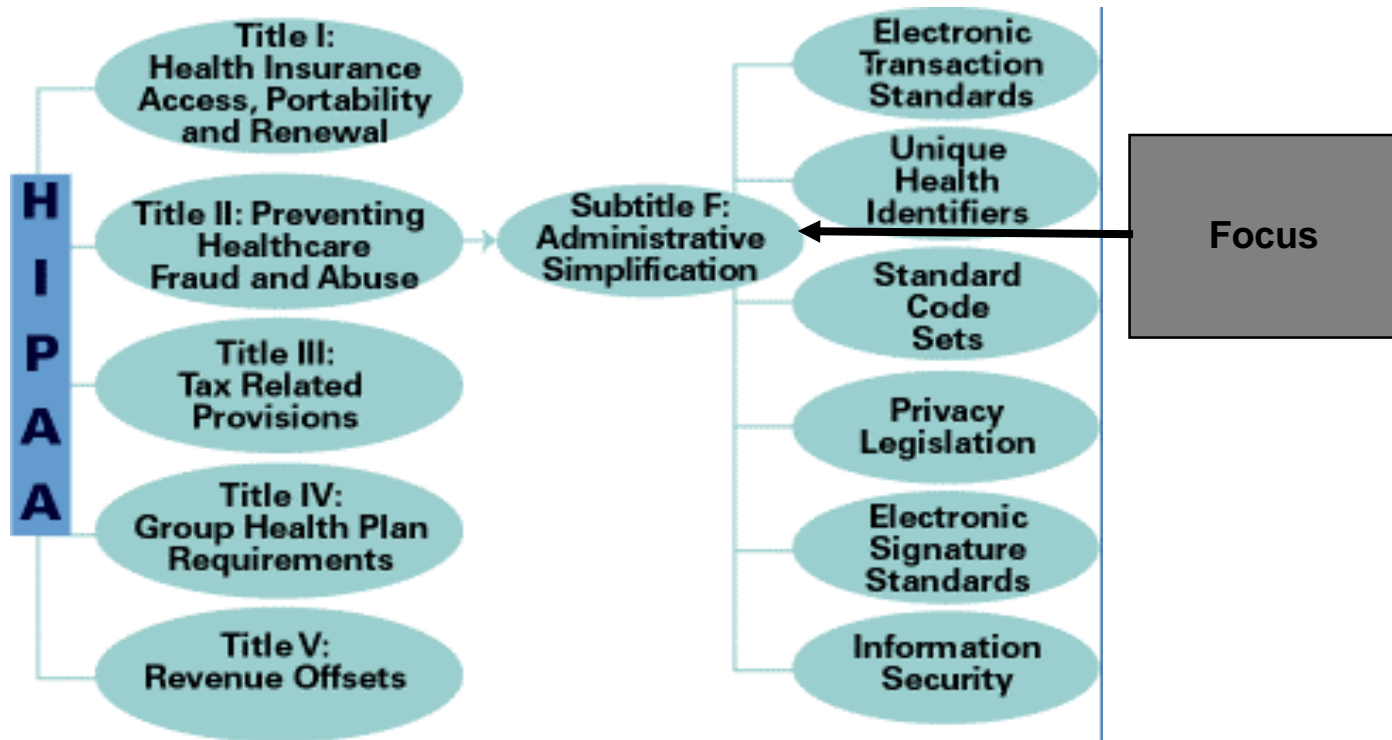
**Robert F. Drewniak**  
**Principal, Arthur Andersen**

**Brett Trusko**  
**Director Strategic Planning**  
**NetFish Technologies**

**October 16, 2000**

# What is HIPAA?

- HIPAA is the Health Insurance Portability and Accountability Act of 1996 (PL 104-191)
- Also referred to as the Kennedy-Kassebaum Act
- HIPAA was enacted by the federal government on August 21, 1996 with the intent to assure health insurance portability, reduce healthcare fraud and abuse, guarantee security and privacy of health information and enforce standards for health information.



## ***When we talk about HIPAA, we are referring to .....***

- Title II, Subtitle F
- Administrative Simplification
  - Data Standardization
    - ✓ Code Sets
    - ✓ Transactions
    - ✓ Identifiers
  - Security
  - Privacy

# ***Data Standardization - Code Sets and Identifiers***

- Proposed Standard Code Sets
  - ICD-9-CM, International Classification of Diseases, 9th Rev., Clinical Modification
  - CPT-4, Physician Current Procedural Terminology
  - Alpha-numeric HCPCS, Healthcare Financing Administration Procedure Code System
  - CDT-2, Current Dental Terminology
  - NDC, National Drug Codes
- Unique identifier numbers have been proposed for providers and employers
- Patients and plan identifiers postponed

# ***Data Standardization - Electronic Transaction Standards***

- Department of Health and Human Services (DHHS) has proposed that the following electronic transactions be standardized:
  - Health care claims or equivalent encounter information.
  - Enrollment and de-enrollment in a health plan.
  - Eligibility for a health plan.
  - Health care payment and remittance advice.
  - Health plan premium payments.
  - Health care claim status.
  - Referral certification and authorizations.
  - Coordination of benefits.
- Standard Claims Attachments
- Electronic Transaction Standard - **X12N** standards facilitate these transactions by establishing a common, uniform business language for computers to communicate across town or around the world.

# *Summary of Proposed Security Requirements*

## – Administrative Security

- Certification
- Contingency plan
- Information access control
- Security configuration management
- Security incident management
- Security management process

## – Physical Data Security

- End user security awareness
- Physical access control
- Media
- Secure workstation use and availability

## – Technical Security

- Access control
- Audit controls
- Authorization control
- Entity authentication

## – Electronic Transmission

- Communication/Network controls

## – Electronic Signatures

- Digital signatures

# ***Summary of Proposed Privacy Requirements***

- Designation of a Privacy Official
- Uses and Disclosure for Treatment, Payment and Health Care Operations
- Minimum Necessary Use and Disclosure
- Right to Restrict or Revoke Use and Disclosure
- Creation of De-identified Information
- Application to Business Partners
- Authorizations initiated by the Individual and the Covered Entity
- Inspection/Copying & Amendment/ Correction of Records by Member
- Notice of Information Practices
- Accounting for Uses and Disclosure
- Uses and Disclosures Permitted Without Member Authorization
- Recordkeeping Requirements
- Training
- Safeguards & Duty to Mitigate
- Internal Complaint Process
- Sanctions

# *Assessment*

- Identify gaps between current technology/practices and the proposed HIPAA requirements.
- Commence an assessment of the gaps and impacts to implement the transactions.
- Identify any translator requirements, if appropriate, and commence the selection process.
- Involve your vendors, clearinghouses and other entities to determine their plans and any assistance that may be available.
- Determine specific plans for implementation of the transactions from both an IS and business perspective.

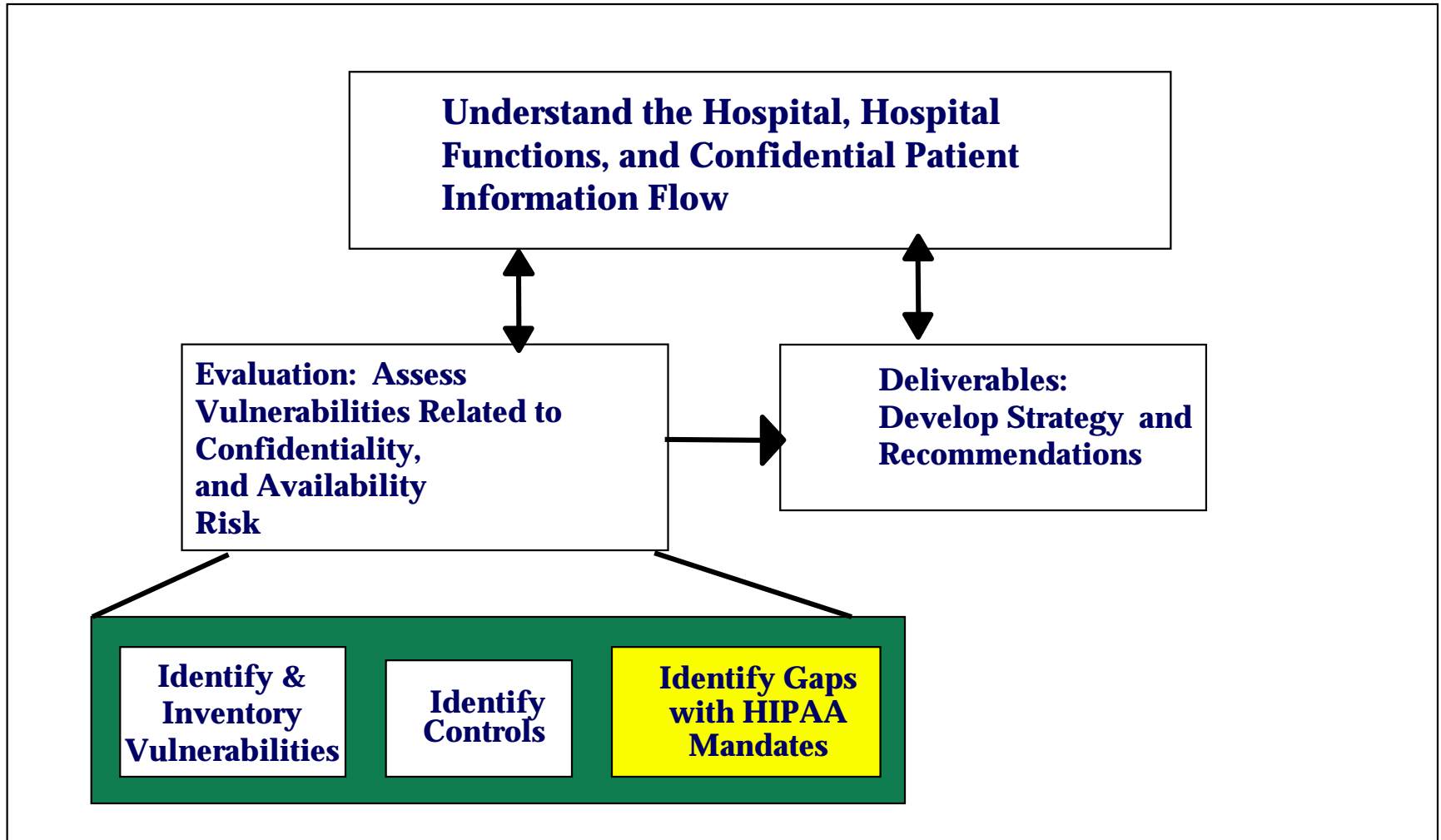
# *Assessment*

- Determine testing criteria and identify your trading partners.
- Develop “Chain of Trust” language to provide to vendors and others, as appropriate.
- Utilize any third party testing tools to determine HIPAA compliance with the Implementation Guides.
- Develop remediation recommendations and a generic, strawman workplan.
- Link HIPAA remediation to existing or planned enterprise-wide initiatives where appropriate.

# *Assessment*

- Review Disaster Recovery Plan
- Review Security and Privacy Policies and Protocols
  - Firewalls - access
  - Passwords, encryption, etc
  - Physical locations of hardware, terminals, fax machines, etc.
- Human Resource Policies
  - Termination procedures
- Training
- Third party arrangements and agreements

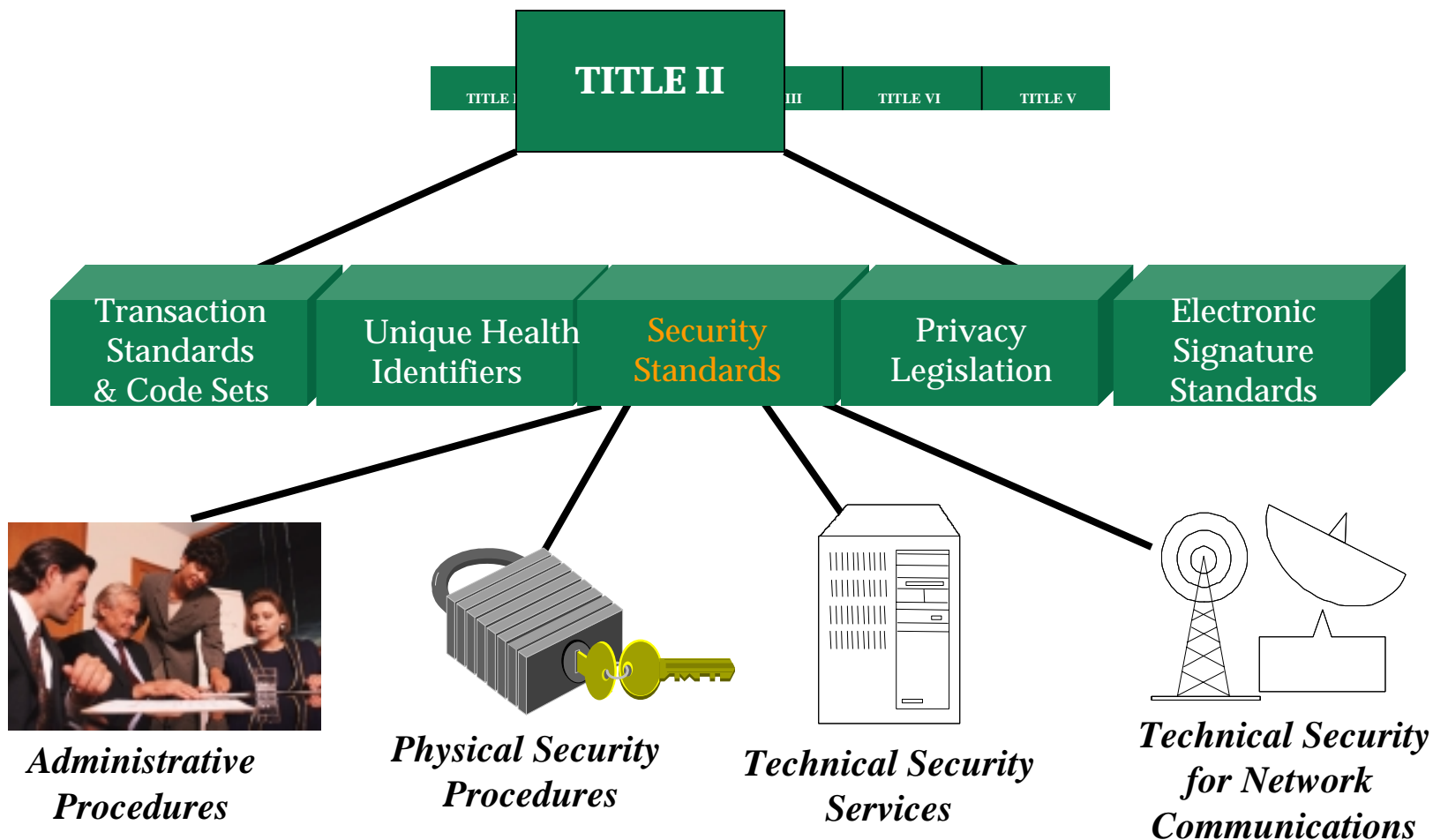
# Assessment



# Next Steps

## Information Protection

Specific information and network security techniques will be required to be implemented to ensure compliance with the Title II mandates including:



# *Next Steps*

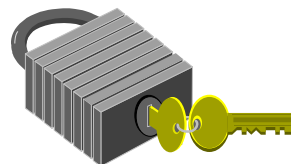
## *Information Protection*



### *Administrative Procedures*

**Organizations will be required to develop and implement administrative security standards relating to:**

- ✓ **Certification**
- ✓ **Chain of Trust Agreements**
- ✓ **Contingency Planning**
- ✓ **Records Processing**
- ✓ **Information Access Control**
- ✓ **Internal Audit**
- ✓ **Personal Security**
- ✓ **Security Configuration Management**
- ✓ **Security Incident Response & Reporting**
- ✓ **Security Management Processes**
- ✓ **Termination Procedures**
- ✓ **Training**



### *Physical Security Procedures*

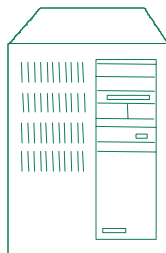
**The following physical safeguards will be necessary:**

- ✓ **Assigned Security Responsibility**
- ✓ **Media Controls**
- ✓ **Physical Access Controls**
- ✓ **Policy/Guideline on Workstation Use**
- ✓ **Secure Workstation Location**
- ✓ **Security Awareness Training**

# *Next Steps*

## *Security Standards*

*Technical  
Security  
Services*



**Organizations will be required to implement the following technical security controls:**

### Access Controls

- ✓ Will require procedures for emergency access.
- ✓ Organizations will also have to choose one control procedure from the following
  - Context Based Access
  - Role Based Access
  - User Based Access
- ✓ Encryption will be optional.

### Authorization Controls

- ✓ Organizations will have to choose one control procedure from the following
  - Role Based Access
  - User Based Access

### Entity Authentication

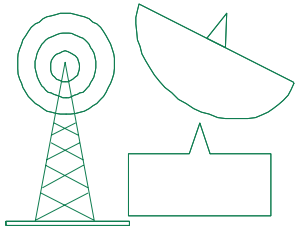
- ✓ Organizations will be required to:
  - Automatic Logoff
  - Unique User Identifiers
- ✓ Organizations will also have to choose one control procedure from the following
  - Biometrics
  - Passwords/PINS
  - Telephone Call Back
  - Tokens

### Data Authentication

Although standards have not yet been set for data authentication, options for control include: Check Sum, Double Keying, Message Authentication, Digital Signatures

# *Next Steps*

## *Security Standards*



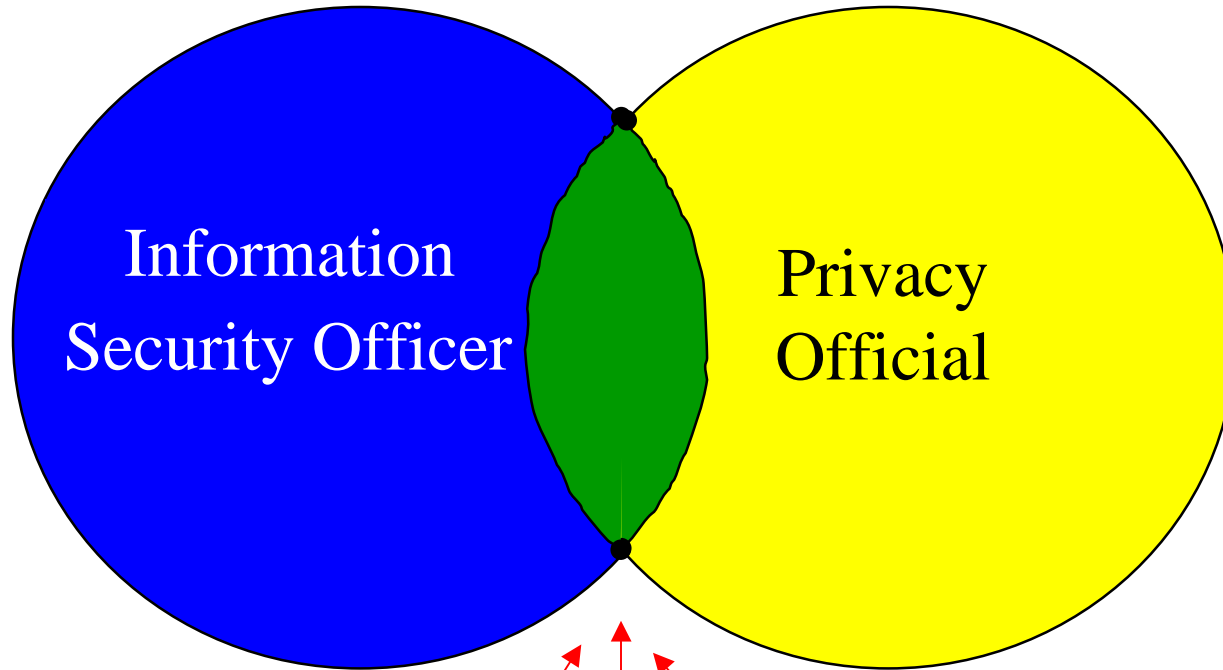
### *Technical Security for Network Communications*

- ✓ Organizations will be required to implement basic networking safeguards and address two (2) network security issues:
  - ☒ Integrity (message corruption) and confidentiality (message interception)
  - ☒ Protection from unauthorized remote access
- ✓ Specifically, organizations will need to implement both integrity controls and message authentication.
- ✓ Organizations will also be required to implement either access controls within their network elements or encryption controls
- ✓ Optional controls organizations can consider include:
  - ☒ Alarms
  - ☒ Audit Trails
  - ☒ Entity Authentication
  - ☒ Event Reporting

## *Next Steps*

- Establish *Internal Sponsorship*
- Establish internal understanding that HIPAA is more than data - 80% privacy, security, policy, procedure, etc.
- Establish HIPAA Governance and Program Management Office
  - Corporate representatives
  - Plan representatives
- Data Standardization - Rules are final. Begin work Now
- Conduct Data Standardization planning sessions to develop approach and drive cost estimates

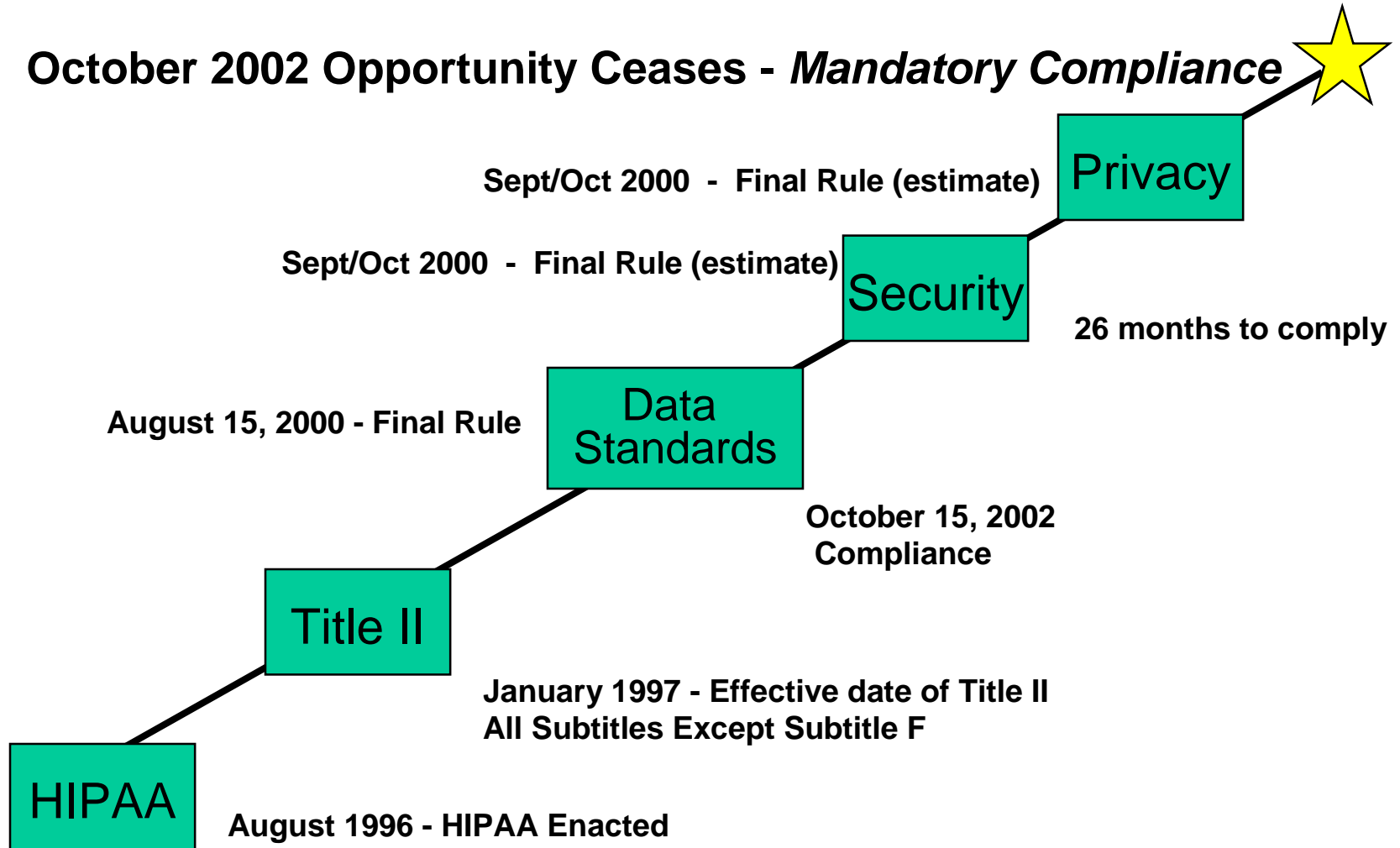
# *Next Steps - Remediation Approach - Security Officer, Privacy Official*



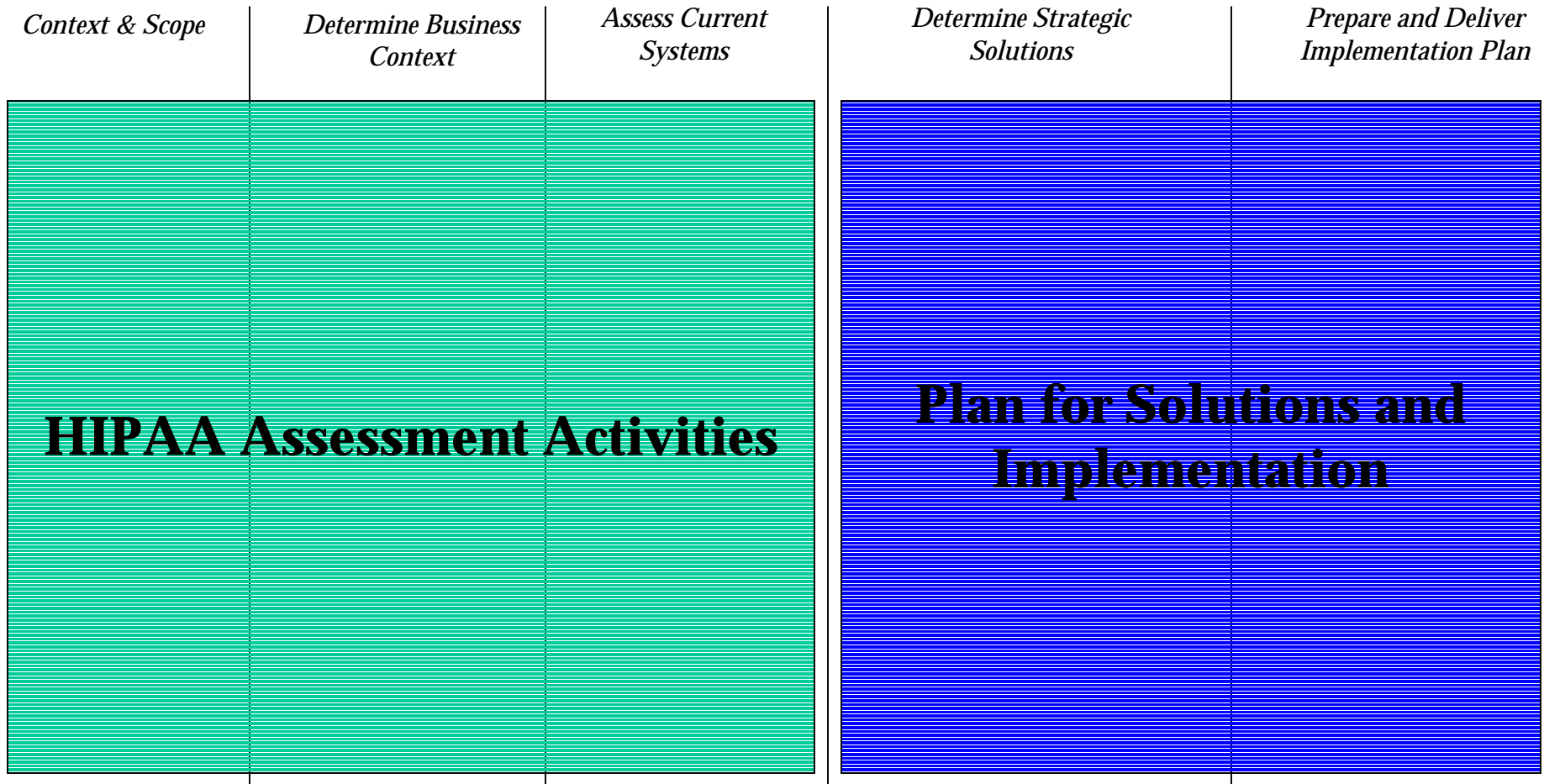
- Policies and procedures
- Chain of trust agreements
- Training materials
- Monitor regulations

# ***HIPAA Timeline***

**October 2002 Opportunity Ceases - *Mandatory Compliance***



# Contextual Approaches to HIPAA



# Now What?

- Transform HIPAA costs into a strategic investment in your e-business strategy
- Assess the opportunity for business process reengineering
- Realign your IT resources to meet the requirements of new standards and an e-business strategy
- Provide a secure, compliant environment for HIPAA and e-commerce information exchange
- Consider an enterprise wide compliance strategy that avoids missed components and costly retrofitting

# HIPAA and E-Business

- The cornerstone of e-business is agreed upon standards for information delivery
- HIPAA delivers the cornerstone
- If e-business is not a part of your HIPAA strategy an important opportunity may be missed

# Business Process E-engineering

- Re-engineering has been replaced with e-engineering
- Businesses will need to understand and e-engineer around electronic processes. The way business has been done in the processing of healthcare transactions is totally different than it will be in the e-business world
- Serious e-engineering requires radical thinking

# Re-align IT Resources

- E-Business requires different approaches to IT
- There is a difference in the “main frame” mentality and the “network mentality”
- Main frame mentality assumes central control and hierarchical solutions, the networked organization requires flat organizations and dynamic management
- Defining business processes around the network is both frightening and exciting

# Provide a Secure Environment

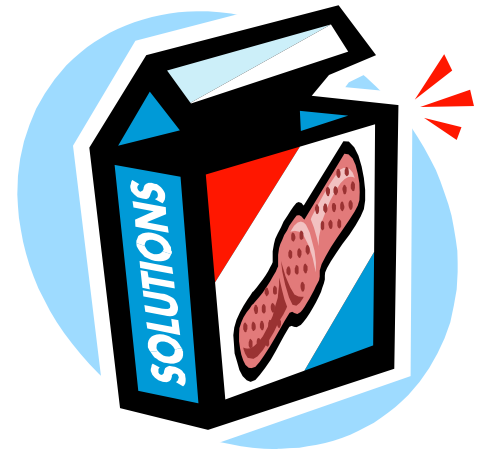
- E-business and HIPAA must go hand in hand. E-business processes, even if outside of the scope of HIPAA should follow HIPAA security guidelines
- Most security breaches in the retail world are internal – ergo the need for security in all transactions and internal processes

# Consider the Entire Enterprise

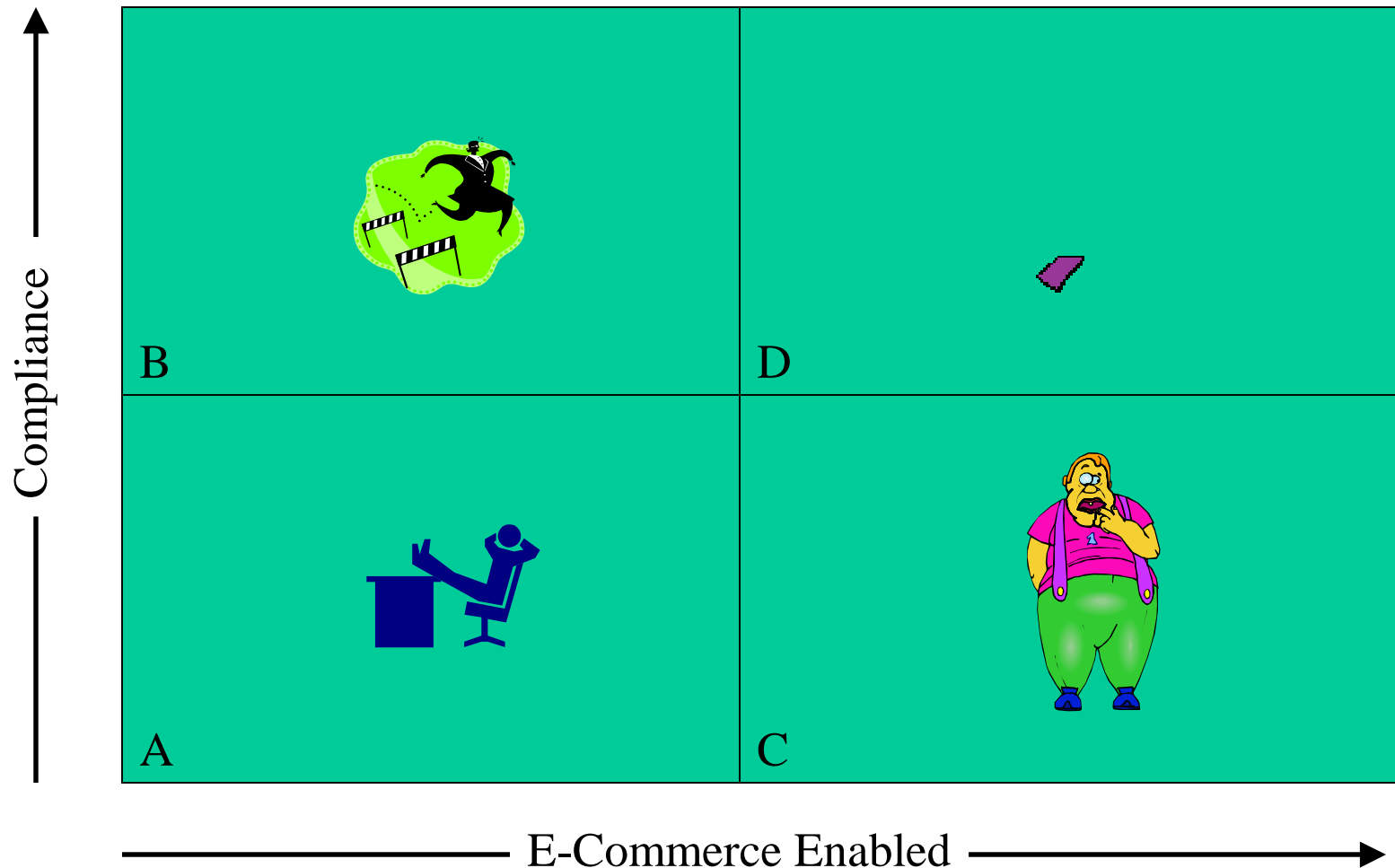
- A solution done halfway will require costly retrofitting
- Consistent with e-business, consider the entire organization as effected by HIPAA

# Determine Solutions

- Many options
- Many solutions providers
- Many plans
- Many actions

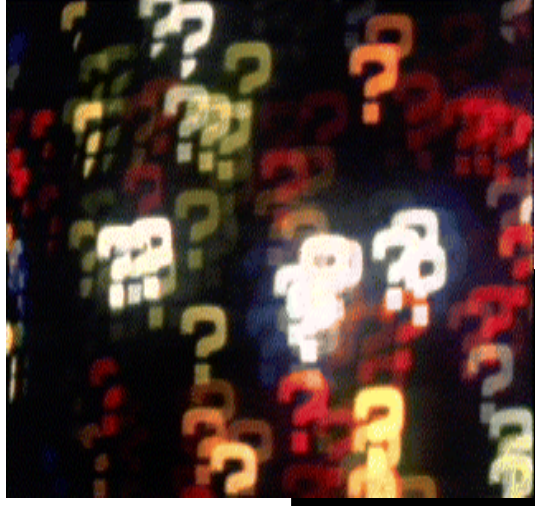


# Evaluate Opportunities



# Conclusions

- X12 EDI is the only acceptable HIPAA data transfer mechanism
- XML and related e-commerce transactions will inevitably be accepted as the language of business
- Healthcare organizations need to plan for X12 compliant transactions in the short term while planning for e-commerce in the future
- HIPAA consultants should have the depth to help an organization plan for both



## Questions & Answers

# End of Presentation