# *HIPAA Security Regulations: Documentation and Procedures*

# The Second National HIPAA Summit

**Healthcare Computing Strategies, Inc.**


**John Parmigiani**
**Practice Director, Compliance Programs**

**Tom Walsh, CISSP**
**Practice Manager, Enterprise Security**

# Presentation Outline

*Many organizations are searching for guidance on how to implement HIPAA Security Standards. This presentation offers some ideas and the policies, procedures and documentation required by HIPAA.*


**Part 1 – Overview – What is HIPAA ..... 1**

Administration Simplification (Diagram)
Security Goals
Observations
HIPAA is More About Change than Technology (Diagram)

**Part 2 – What is Required ..... 2**

Policies, Procedures, Forms & Memos (Diagram)
Security Policies
Administrative Procedures (Table)
Physical Safeguards (Table)
Technical Security (Table)
Transmission Security (Table)

**Elements of a Security Program (Diagram & Table) ..... 5**

**Part 3 – Getting Started ..... 6**

Roles and Responsibilities
Security Planning
Policies and Procedures
Workstations
Media Controls (CIA)

**Part 4 – Implementation ..... 8**

Certification of Systems
Training, Education and Awareness (TEA)
Configuration Management
Incident Report and Handling

**Part 5 – Changing the Culture ..... 9**

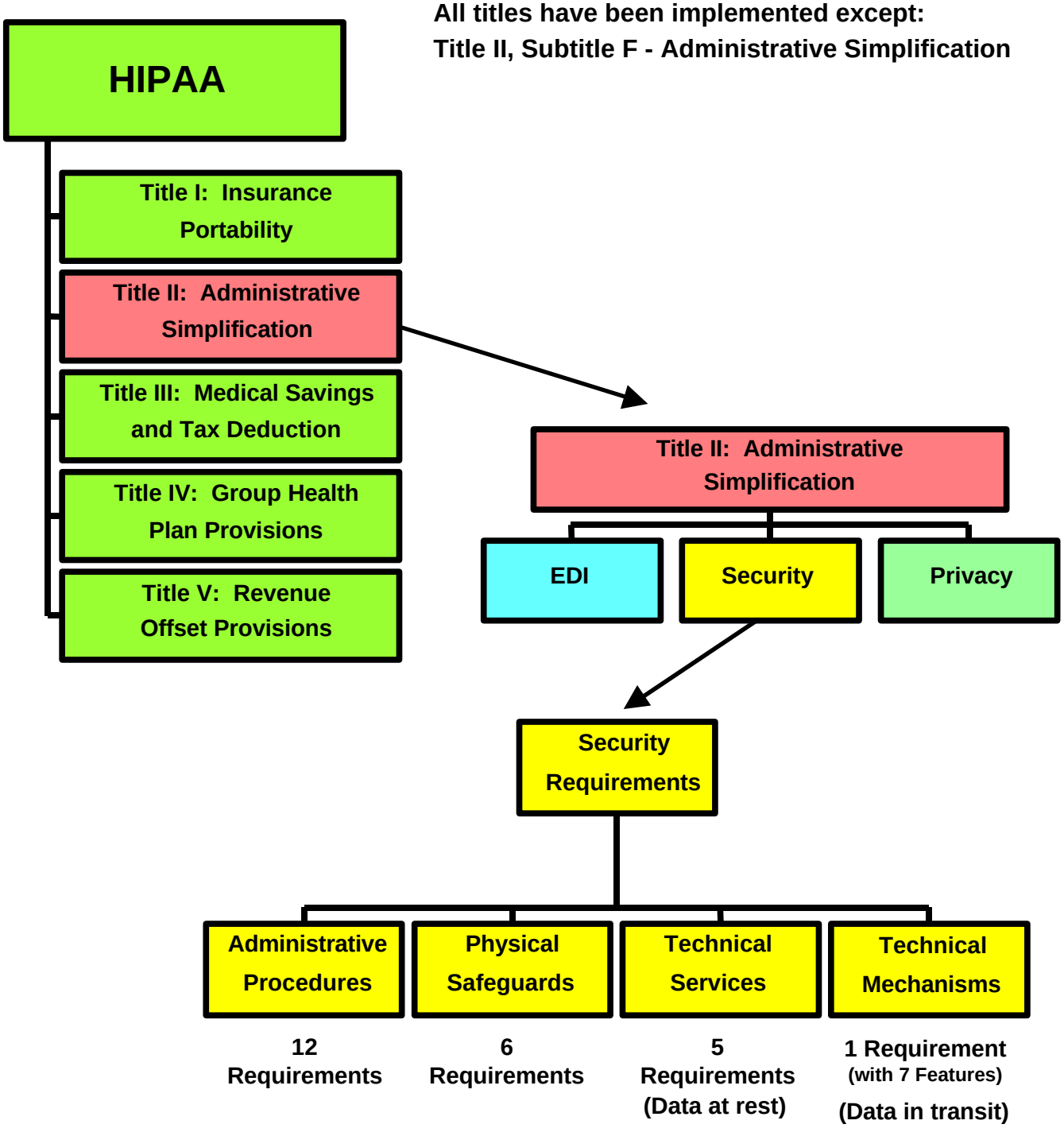
Today's Situation
Resource Considerations

**Part 6 – Conclusion ..... 9**

# 1. Overview – What is HIPAA?

*The Health Insurance Portability and Accountability Act of 1996 (HIPAA)*
*Public Law 104-191*

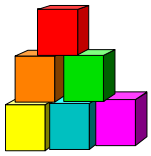
**All titles have been implemented except:**
**Title II, Subtitle F - Administrative Simplification**



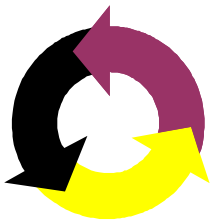
## Security Goals

*Is security a business enabler or an expense?*

- Confidentiality
- Integrity
- Availability

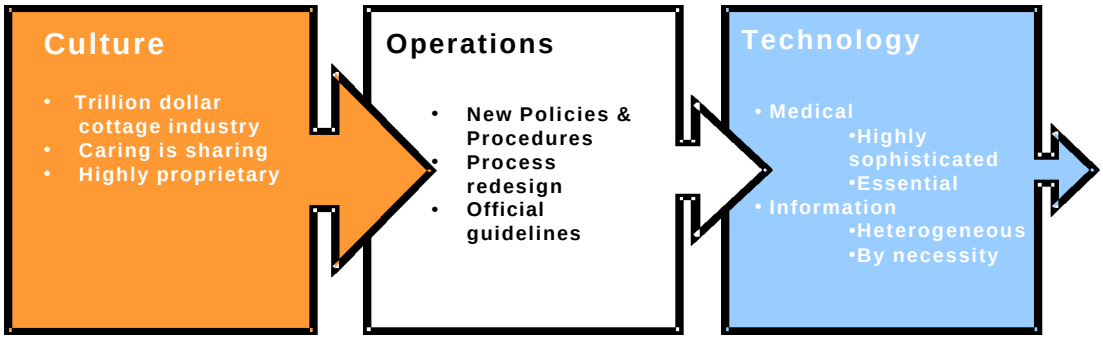


## Observations

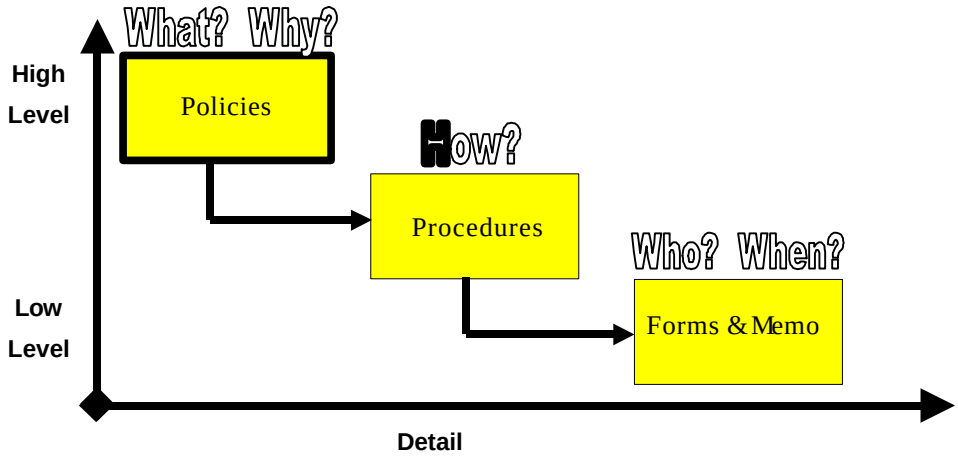


- Cannot attempt to impose monolithic “solutions”
- Continuous development process
- “Two Year” Requirement - Opportunity for assessment
- Need for a “Best Practices” document

## HIPAA is More About Change, than Technology




# 2. What is Required



# Security Policies

**Administrative**
- Formal mechanism for processing records
- Information access control
- Sanction Policy

**Physical**
- Assigned security responsibility
- Media controls
- Physical access controls
- Workstation use

**Technical**
- Authorization control

| Administrative Procedures | Policy | Proc. | Form | Memo |
|---|---|---|---|---|
| **Certification** | | **X** | **X** | |
| **Chain of trust partner agreement** | | | **X** | |
| **Contingency plan** | | **X** | | |
| Disaster Recovery | | X | | |
| Emergency Mode Access Procedures | | X | | |
| **Formal mechanism for processing records** | **X** | | | |
| Release of Information | | | X | |
| Confidentiality Agreements | | | X | |
| **Information access control** | **X** | | | |
| Request for UserID & Password | | X | X | |
| Role-Based Authorization | | X | | |
| **Internal audit** | | **X** | | |
| **Personnel security** | | **X** | | |
| Clearances (Background Checks) | | | X | |
| **Security configuration management** | | **X** | | |
| Change Control | | X | X | |
| Inventory (Property Pass) | | X | X | |
| Security Testing | | X | X | |
| **Security incident procedures** | | **X** | **X** | |
| **Security management process** | | **X** | | |
| Security Policy (Overall) | X | | | |
| Risk Analysis & Management | | X | X | |
| Sanction Policy | X | | | X |
| **Termination procedures** | | **X** | | |
| Exit Interview Checklist | | | X | |
| **Training** | | **X** | | |
| Attendance Sheet, Test, etc. | | | X | |

## Required Policies, Procedures, and Documents (Continued)

| Physical Safeguards | Policy | Proc. | Form | Memo |
|---|---|---|---|---|
| **Assigned security responsibility** | **X** | | | **X** |
| **Media controls** | **X** | **X** | | |
| Accountability (Liability Agreements) | | X | X | |
| Backups | | X | | |
| Disposal | | X | | |
| **Physical access controls** | **X** | | | |
| Escort procedures | | X | | |
| Visitor sign-in log sheet | | | X | |
| **Policy/guideline on workstation use** | **X** | | | |
| **Secure workstation location** | | **X** | | |
| **Security awareness training** | | **X** | **X** | **X** |

| Technical Security | Policy | Proc. | Form | Memo |
|---|---|---|---|---|
| **Access control** | | **X** | | |
| Procedure for Emergency Access | | | X | |
| **Audit controls** | | **X** | | |
| Logs | | | X | |
| **Authorization control** | **X** | **X** | | |
| Request for UserID and System Access | | | X | X |
| **Data authentication** | | **X** | | |
| **Entity authentication** | | **X** | | |

| Transmission Security | Policy | Proc. | Form | Memo |
|---|---|---|---|---|
| **Communications/network controls** *(Access controls, Alarm, Audit trail, Encryption, Entity authentication, Event reporting, Integrity controls, Message authentication.)* | | **X** | | |

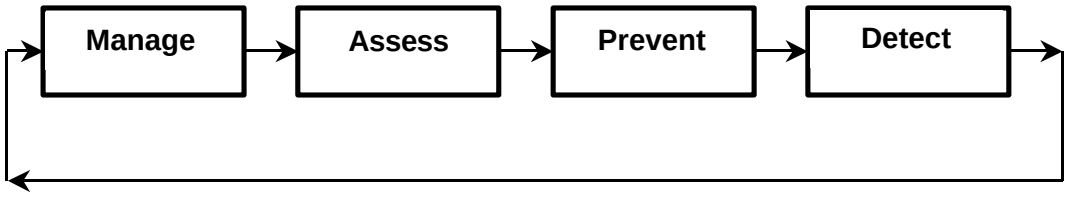
***Optional:***

Software Use
Modem Use
Internet and E-Mail Usage
Classification of Information (Assignment of Data Ownership)

# Elements of a Security Program

*"Secure your enterprise and compliance will follow." – Steve Hunt, GIGA 12/99*

**Four Cycle Process:**




| | | |
|---|---|---|
| **Manage** | 1. | Roles and Responsibilities |
| (Planning and hiring) | 2. | Security Planning |
| | 3. | Policy and Procedures |
| | 4. | Security Management |
| **Assess** | 5. | Risk Assessment |
| (Organizing) | 6. | PC Workstation Security (Laptop & Portable) |
| | 7. | Systems Security (Servers & Mainframes) |
| | 8. | Communication Security (Network) |
| | 9. | Software (Operating System & Application) |
| | 10. | Media Controls & Information Security |
| **Prevent** | 11. | Certification of Systems |
| (Directing) | 12. | Training, Education & Awareness |
| | 13. | Physical & Personnel Security |
| | 14. | Access Control (Physical, Logical, & Remote) |
| | 15. | Configuration Management |
| | 16. | Contingency & Disaster Recovery |
| **Detect** | 17. | Audit Trails |
| (Controlling) | 18. | Audit Controls & Alarms |
| | 19. | Incident Reporting & Handling |
| | 20. | Program Review (Internal Audit) |

*The real threat lies not necessarily in the distant chance of the interception of patient information in transmission, but the storage and management of the information once it is received. Encrypting patient information during transmission is "due diligence." But once the information is received and decrypted, what level of protection is applied to the information?*

# 3. Getting Started

## Roles and Responsibilities

- Assign Security Responsibility
  - Information Security Manager / Officer
  - Privacy Officer
- Assignments _____
- Responsibilities include:
  1) The use of security measures
  2) The conduct of personnel
- Establish a _____

**Question:** ***What attributes do you think a good security manager needs?***

_____

_____

## Security Planning

- Brief management and leadership on HIPAA and its impacts
- Establish a _____
- Determine resources required:
  Budgets, staff, equipment, etc.

## Policies and Procedures

- Review and update existing policies and procedures
- Create new policies and procedures

**Question:** ***What are the fallacies of policy?***

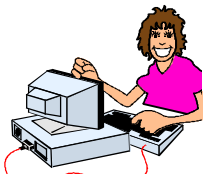
_____

_____

## Workstations (Then and Now…)

| | | |
|---|---|---|
| **Hardware** | **Mainframes & Terminals** | |
| **Software** | **Custom Designed** | |
| **Location** | **Centralized** | |
| **Support** | **Few; Highly Skilled** | |
| **Malicious Code** | **Few** | |
| **Misuse & Abuse** | **Rare** | |

## Guideline on Workstation Use (Includes laptops)



Documented instructions/procedures delineating the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings, of a specific computer terminal site or type of site, dependant upon the sensitivity of the information accessed from that site.

*Part of Physical safeguards to guard data integrity, confidentiality, and availability on the matrix.*

- Information protection (Log off)
- File storage and deletion
- Disposal procedures
- Monitor position

*"Donut Strike"*

## Media Controls (CIA)

***CIA =*** *Confidentiality, Integrity, & Availability*

- Controlled access to media
  (EX: Patient information stored on a server)
- Accountability – Liability Agreements
- Data backup, storage and _____

## Protecting Patient Information

- Printed
- Faxed
- Stored
  Paper and electronic media
- Transmitted

# 4. Implementation

## Certification of Systems

### What?

The technical evaluation performed as part of, and in support of, the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements. This evaluation may be performed internally or by an external-accrediting agency.

*Part of administrative procedures to guard data integrity, confidentiality, and availability.*

## Training, Education and Awareness (TEA)

- **Training** = _____
- **Education** = _____
- **Awareness** = _____

***The goal of TEA – Changing Behaviors***

*What is the difference?*

## Configuration Management

- Documentation
- Change control
- Security Testing (After significant changes to system)
- Anti-virus updates

**Question:** ***Are there procedures for the implementation of software patches and security advisories?***

## Incident Report and Handling

*Can associates identify an unauthorized use of patient information?*

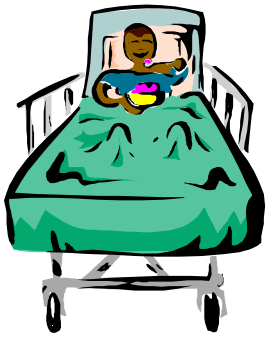
*Do associates know how to report security incidents?*

*Will associates report an incident?*

*Do those investigating security incidents know how to preserve evidence?*

# 5. Changing the Culture

## Today's Situation



- Limited resources for security
- Privacy is not a market differentiator
- Most believe _____
- Up until HIPAA, few incentives for security

**Question:** ***How long does it take to change an organization's culture?***

## Resource Considerations

- **Time** - 26 months from final rule posting
- **Money** - Cost of compliance unknown
- **People** - Skilled staff in EDI and security
- **Vendors** - Hardware and software

# 6. Conclusion

- **Determine what are the policies, procedures, and forms your organization will use to prove compliance.**
- **Get started now by building a good security program and HIPAA compliance will follow.**
- **Everyone is still struggling along - No organization can claim to be "compliant" because the final rules are not published.**

*Thanks for attending!*

*It is our hope that this presentation served your needs. We welcome your feedback. If we can be of help to you in the future, please contact us at:*

**E-mail:** jcparmigiani@hcs-is.com **Voice:** (410) 750-2060

**E-mail:** trwalsh@hcs-is.com **Voice:** (913) 696-1573