Preconference III: Basic Strategies to Comply with the HIPAA Security Rule

~Introduction and Overview~

John Parmigiani

Senior Vice President for Consulting Services

QuickCompliance, Inc.

John Parmigiani

- QuickCompliance, Inc. Senior Vice President for Consulting Services
- President, John C. Parmigiani & Associates, LLC
- CTGHS National Practice Director for Regulatory and Compliance Services
- HCS Director of Compliance Programs
- HIPAA Security Standards Government Chair/ HIPAA Infrastructure Group
- Directed development and implementation of security initiatives for HCFA (now CMS)-Director of Enterprise Standards
  - Security architecture
  - Security awareness and training program
  - Systems security policies and procedures
  - E-commerce/Internet
- Directed development and implementation of agency-wide information systems, policy, and standards and information resources management
- AMC Workgroup on HIPAA Security and Privacy;Content Committee of CPRI-HOST/HIMSS Security and Privacy Toolkit; Editorial Advisory Boards of *HIPAA Compliance Alert's HIPAA Answer Book* and *HIPAA Training Line, HIPAA Training Alert, and Health Information Compliance Alert;* Chair,*HIPAA-Watch* Advisory Board; *Train for HIPAA* Advisory Board; *Train for Compliance* Board of Directors; HIMSS Privacy and Security Steering Committee; JCAHO/NCQA Privacy Certification Committee for Business Associates; Frequent speaker at national conferences

Session Overview

- **HIPAA Security 101**
  - Lesley Berkeyheiser & Sue Miller
- **Six+ Months to Go: Tuning Up for Security Compliance – Tips of the Trade**
  - Holt Anderson
- **Simplifying the Administration of HIPAA Security: A Practical Approach**
  - Angel Hoffman
- **Security Standards Workshop: An Overview - from Risk assessment to Proposed Policies**
  - **Frank Ruelas**
- **Q&As after each and, if needed, at the end**

Our Goal

- To provide you with a thorough understanding of what's expected for compliance with the HIPAA Security Rule
- To share with you some practical implementation advice as you work toward compliance by April 21, 2005
- To discuss our views on what we believe might be "reasonable" and "appropriate" and to attempt to demystify the regulation

HIPAA (AS) Intent

- **Reduce healthcare administrative costs by standardizing (format and content) electronic data interchange (EDI) for claims submission, claims status, referrals, eligibility, COB, attachments, etc.- Foster E-Commerce - can also be used to streamline ordering and paying for supplies and services**
- **Establish patient's right to Privacy**
- **Protect patient health information by setting and enforcing Security Standards**
- **Promote the attainment of a complete Electronic Medical Record (EMR)**

HIPAA Characteristics

- HIPAA is forever and compliance is an ever-changing target
- HIPAA is more about process than technology
- HIPAA is about saving $$ and delivering improved healthcare
- HIPAA is policy-based (documentation is the key)
- HIPAA advocates cost-effective, reasonable solutions
- HIPAA should be applied with a great deal of "common sense"

Administrative Simplification Trilogy

- **Transactions and Code Sets (TCS)**
  - October 16, 2003 compliance date>>>…
- **Privacy**
  - April 14, 2003 compliance date
- **Security***
  - April 21, 2005 compliance date

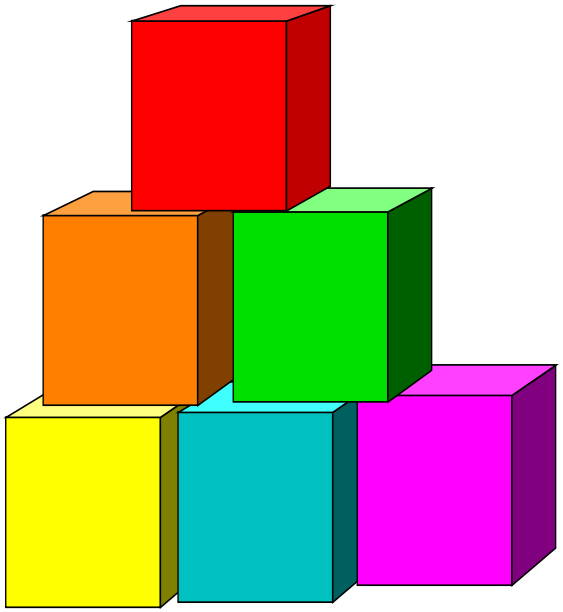
**** the last piece, finally!***

HIPAA Security Rule Intent

- **Ensure the confidentiality, integrity,and availability (CIA) of all electronic protected health information (PHI)**
- **Protect against any reasonably anticipated threats and uses or disclosures that are not allowed by Privacy**
- **Mitigate these threats by whatever safeguards you believe can reasonably and appropriately be implemented in line with the Security Rule standards**

Security Goals

- **Confidentiality**
- **Integrity**
- **Availability**



of protected health information

Good Security Practices

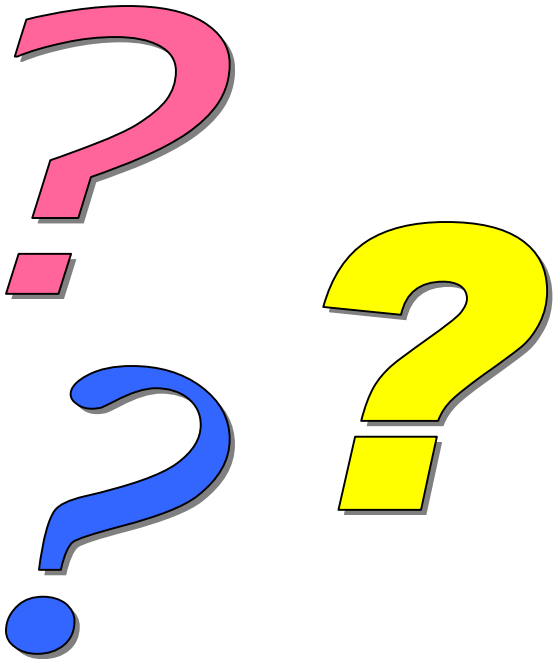
- **Access Controls- restrict user access to PHI based on need-to-know**
- **Authentication- verify identity and allow access to PHI by only authorized users**
- **Audit Controls- identify who did what and when relative to PHI**

Any enforcement of the regulation will focus on how well you are doing these!

Terminology

What did the government really mean when it used the following words:

- **Ensure**
- **Thorough**
- **Audit**
- **Addressable**
- **Reasonable**
- **Appropriate**



Two Themes

- First two presentations deal with what the regulation intends and some of the implications that you should be aware of as you work toward compliance
- The last two presentations take what was discussed in the first two and apply it in real-life covered entity environments

Our First Presentation

- **HIPAA Security 101**
  - **Lesley Berkeyheiser**
    - **Principal, The Clayton Group**
    - **Co-chair, WEDI SNIP Security & Privacy Workgroup**
  - **Sue Miller,Esq.**
    - **Director, Health Transformation Solutions, Webify Solutions, Inc.**
    - **Co-chair, WEDI SNIP Security & Privacy Workgroup**