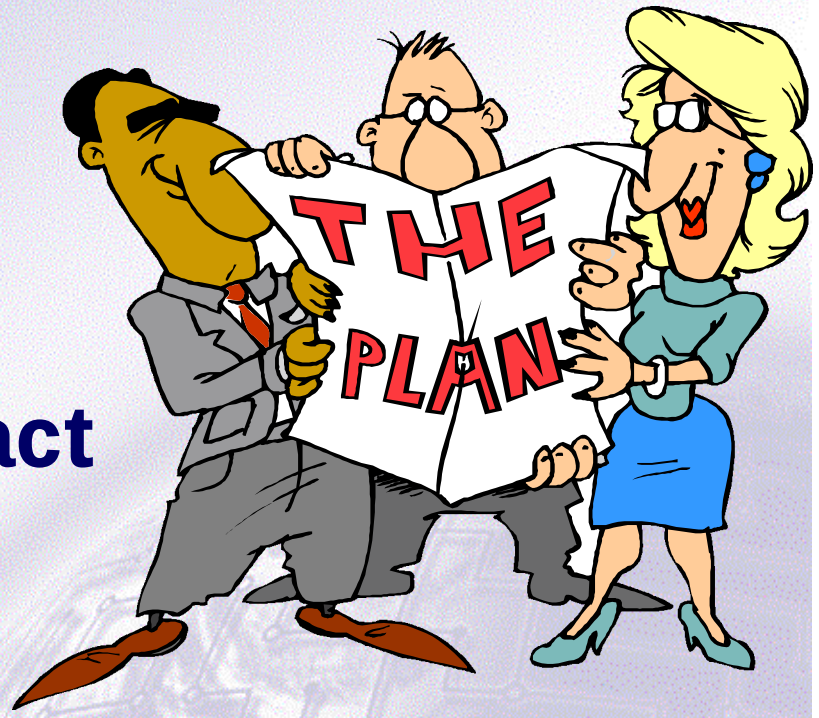

ctg
HealthCare
Solutions

HIPAA Security

John Parmigiani
Director
HIPAA Compliance Services
CTG HealthCare Solutions, Inc.

Presentation Outline

- Introduction
- Overview of HIPAA Security and its Impact
- The Final Rule?
- Conclusions



Introduction

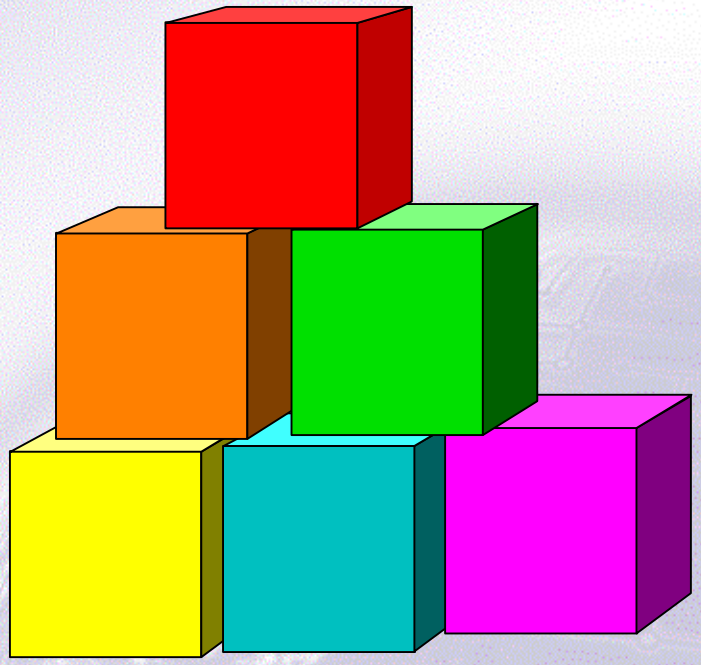
John Parmigiani

- CTGHS Director of HIPAA Compliance Services
- HCS Director of Compliance Programs
- HIPAA Security Standards Government Chair / HIPAA Infrastructure Group
- Directed development and implementation of security initiatives for HCFA
  - Security architecture
  - Security awareness and training program
  - Systems security policies and procedures
- 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 Security and Privacy Toolkit; Editorial Advisory Board of *HIPAA Compliance Alert's HIPAA Answer Book*

Overview of HIPAA Security & its Impact

Security Goals

- Confidentiality
- Integrity
- Availability



HIPAA Security Framework

Flexible-Scalable-Technology Neutral

- **Each affected entity must assess own security needs and risks**

&

- **Devise, implement, and maintain appropriate security to address business requirements**

Security Standards

- **What do they mean for covered entities?**
  - **Procedures and systems must be updated to ensure that health care data is protected.**
  - **Written security policies and procedures must be created and/or reviewed to ensure compliance.**
  - **Employees must receive training on those policies and procedures.**
  - **Access to data must be controlled through appropriate mechanisms (for example: passwords, automatic tracking of when patient data has been created, modified, or deleted).**
  - **Security procedures/systems must be certified (self-certification is acceptable) to meet the minimum standards.**

Security Compliance Areas:

- Training and Awareness
- Policy and Procedure Review
- System Review
- Documentation Review
- Contract Review
- Infrastructure and Connectivity Review
- Access Controls
- Authentication
- Media Controls

Security Compliance Areas…:

- Workstation
- Emergency Mode Access
- Audit Trails
- Automatic Removal of Accounts
- Event Reporting
- Incident Reporting
- Sanctions

Security Measures

In general, security measures can grouped as:

- Administrative
- Physical
- Technical (Data in transit and data at rest)

Security Standards

- **NPRM- 8/12/1998**
  - **Administrative Requirements (12)**
  - **Physical Requirements (6)**
  - **Technical Requirements [data at rest](5)**
  - **Technical Requirements [data in transit](1)**
  - **Electronic Signature**
  - **Implementation Features (70)**

BS 7799 / ISO 17799

- Security Policy
- Security Organization
- Asset Classification and Control
- Personnel Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Systems Development and Maintenance
- Business Continuity Management
- Compliance

Standard Areas of Business Security

Security – The Privacy Rule

- **164.530 (c)**
  - **Standard: safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information**
  - **Implementation specification: safeguards. A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.**

HIPAA Statutory- Security [USC 1320d-2(d)(2)]

"Each covered entity who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards : (A) to ensure the integrity and confidentiality of the information; and (B) to protect against any reasonably anticipated (i) threats or hazards to the security or integrity of the information; and (ii) unauthorized uses or disclosures of the information; and (C) otherwise to ensure compliance with this part by the officers and employees of such person"

Is in Effect Now!

The Final Rule?

HIPAA Security-The Final Rule

- Final Rule in clearance- expected to be published summer (Q3) 2002
- What to expect
  - Streamlining- Same core values- more specificity as to mandatory (must do)/discretionary (should do)
  - Fewer standards
  - Paper (?) as well as electronic media
  - Business Associate Contracts/Chain-of-Trust
  - Synchronization with Privacy
- What not to expect
  - No Electronic Signature but…not dead for health care

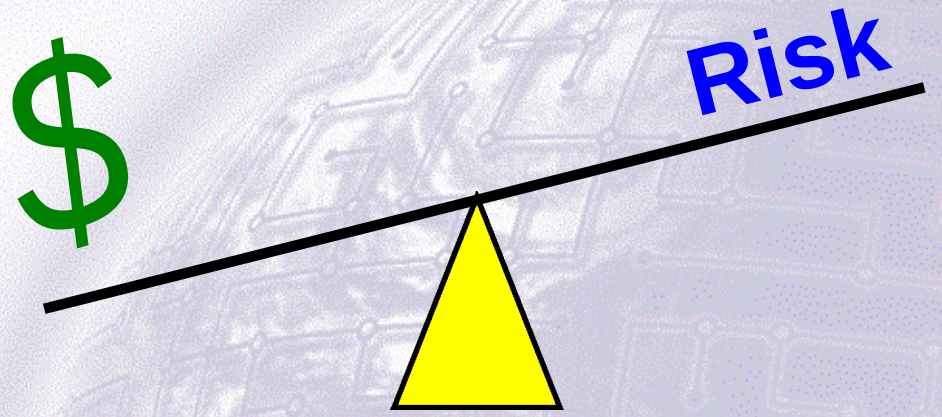
Electronic Signature Standard

- Comments to Security NPRM indicated a lack of consensus; industry continues to work on, monitored by NCVHS
- NCVHS necessary before regulation developed
- Transaction standards do not require
- Security NPRM specified digital signature (authentication, message integrity, non-repudiation requirements)
- NIST rather than DHHS will probably develop
- PKI-HealthKey Bridge effort / interoperability problems

Conclusions

A Balanced Approach

- Cost of safeguards vs. the value of the information to protect
- Security should not impede care
- Your organization's risk aversion
- Due diligence



Reasonableness/Common Sense

- **Administrative Simplification Provisions are aimed at process improvement and saving money**
- **Healthcare providers and payers should not have to go broke becoming HIPAA-compliant**
- **Expect fine-tuning adjustments over the years**

Remember:

Due Diligence!

Thank You

Questions?

john.parmigiani@ctghs.com / 410-750-2497