Implementing and Enforcing the HIPAA Security Rule

John Parmigiani
National Practice Director
Regulatory and Compliance Services
CTG HealthCare Solutions, Inc.

Presentation Overview

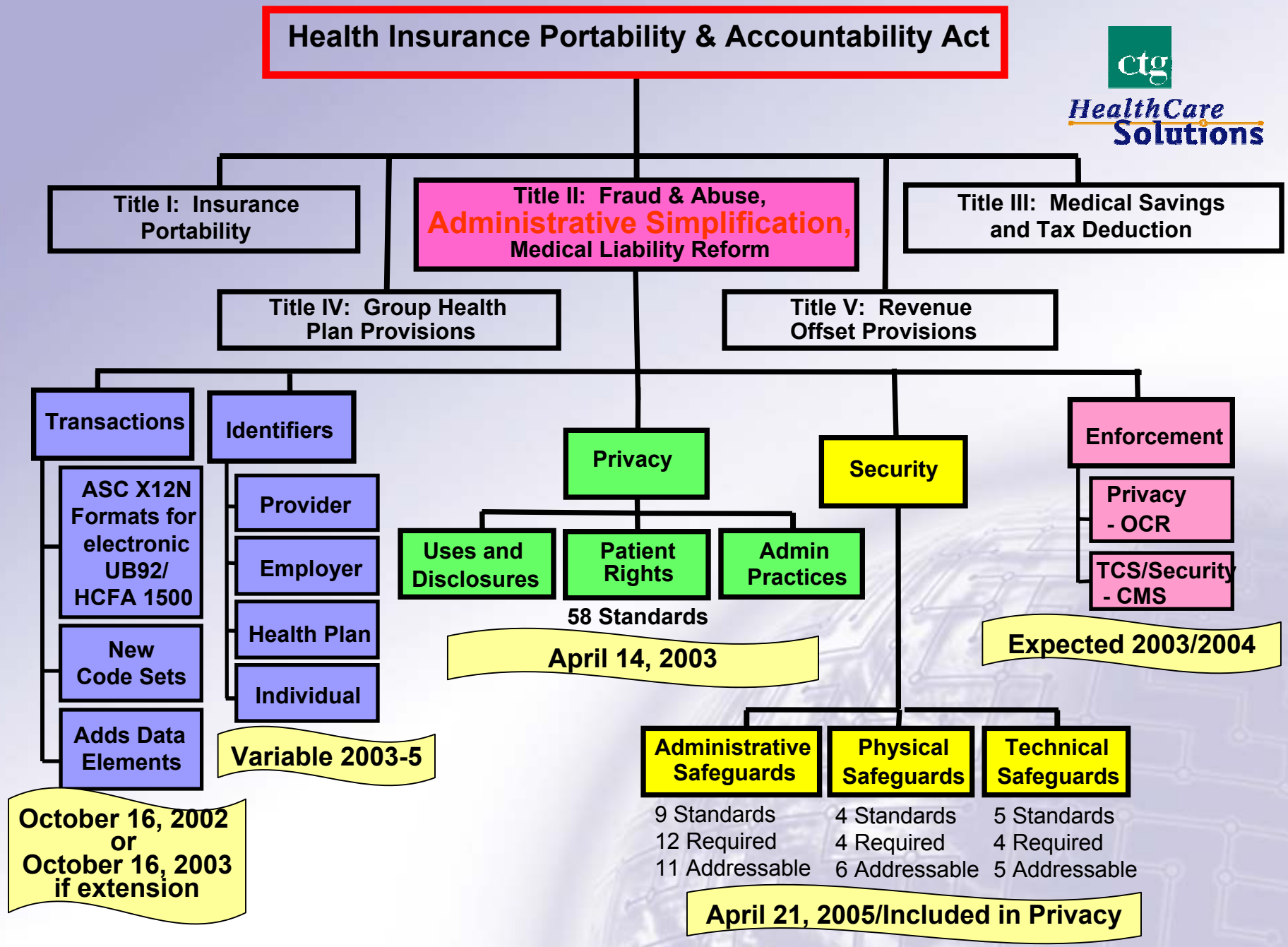
- Introductions
- Final Security Rule
  - How we got there
  - Comparison to NPRM
  - Key Concepts
  - Steps Toward Compliance
- Enforcement

Introductions

John Parmigiani

ctg HealthCare Solutions

- CTGHS National Practice Director for Regulatory and Compliance Services
- CTGHS National Practice 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 (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;* Chair,*HIPAA-Watch* Advisory Board; *Train for HIPAA* Advisory Board; HIMSS Privacy and Security Task Force


Health Insurance Portability & Accountability Act
ctg
HealthCare Solutions
Title I: Insurance Portability
Title II: Fraud & Abuse, Administrative Simplification, Medical Liability Reform
Title III: Medical Savings and Tax Deduction
Title IV: Group Health Plan Provisions
Title V: Revenue Offset Provisions
Transactions
ASC X12N Formats for electronic UB92/ HCFA 1500
New Code Sets
Adds Data Elements
October 16, 2002 or October 16, 2003 if extension
Identifiers
Provider
Employer
Health Plan
Individual
Variable 2003-5
Privacy
Uses and Disclosures
Patient Rights
Admin Practices
58 Standards
April 14, 2003
Security
Administrative Safeguards
Physical Safeguards
Technical Safeguards
9 Standards
12 Required
11 Addressable
4 Standards
4 Required
6 Addressable
5 Standards
4 Required
5 Addressable
April 21, 2005/Included in Privacy
Enforcement
Privacy - OCR
TCS/Security - CMS
Expected 2003/2004

Final Security Rule-how we got there

HIPAA Security Standards (NPRM)

- Government / Industry Cooperation
- Industry Self-Regulation
- Continuous Development Process
- Best Practices

HIPAA Security Framework (NPRM)

ctg HealthCare Solutions

Flexible-Scalable-Technology Neutral-Comprehensive

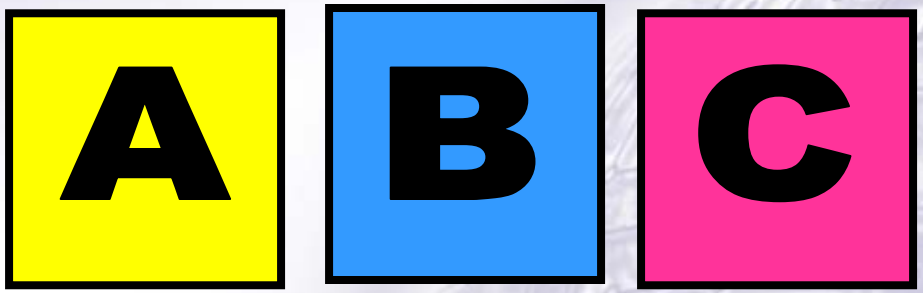
- **Each affected entity must assess own security needs and risks**

&

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

HIPAA Security Standards (NPRM)

- Are based upon good business practices;
- Tell you what to do, not how to do it; and
- Are listed in alphabetical order.



HIPAA = Culture Change

ctg HealthCare Solutions

Organizational culture will have a greater impact on security than technology.

20% technical

80% policies & procedures

Must have people optimally interacting with technology to provide the necessary security to protect patient privacy. Open, caring-is-sharing environment replaced by "need to know" to carry out healthcare functions.

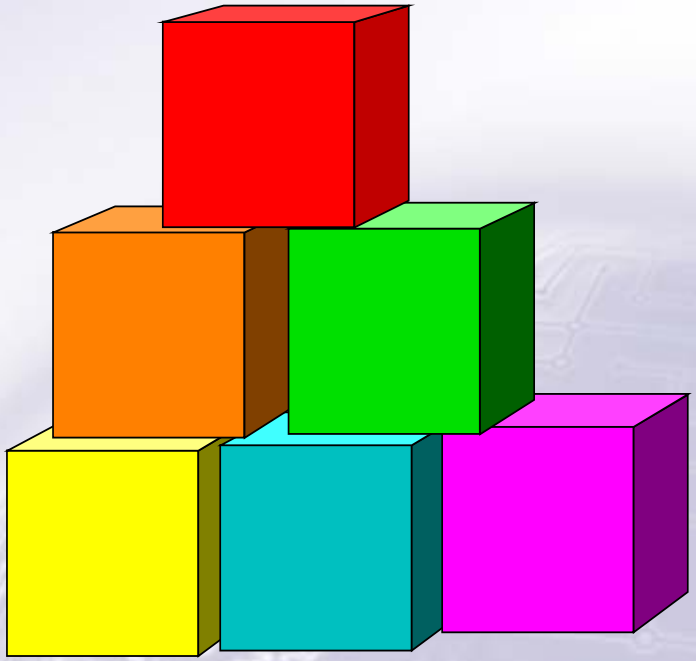
Security: Getting Started (NPRM)

ctg HealthCare Solutions

- Appoint Security Officer
- Establish policies and procedures
- Train staff and enforce policies
- Implement physical access controls
- Provide for authentication of users
- Install adequate technical security controls such as firewalls and audit trails
- Configuration management for installing and maintaining hardware and software

Security Goals

- Confidentiality
- Integrity
- Availability



of protected health information

Good Security Practices

ctg HealthCare Solutions

- **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**

Final Security Rule- Comparison to NPRM

Comparison of Rules

ctg HealthCare Solutions

Old Proposed Rule –

- 24 Requirements
- 69 Implementation Features

New Final Rule –

- 18 Standards
- 42 Implementation Specifications:
  - 20 Required
  - 22 Addressable

Comparison of Rules

Old Proposed Rule –

- Section headings, Requirements and Implementation Features were listed in alphabetical order so as not to imply the importance of one requirement over another

New Final Rule –

- Standards and Implementation Specifications are grouped in a logical order within each of the three areas: *Administrative, Physical and Technical Safeguards*

Other Changes

- Removes the Electronic signature standards
- Incorporates standards that parallel those in the Privacy Rule thus helping organizations meet a number of the security standards through the implementation of the privacy rule (Safeguards)
- Covers only electronic protected health information *(More limited than Privacy Rule)*
- Requires a minimum level of documentation that must be periodically updated to reflect current practices

HIPAA Security Standards

- **Administrative (55%)**
  - 12 Required, 11 Addressable
- **Physical (24%)**
  - 4 Required, 6 Addressable
- **Technical (21%)**
  - 4 Requirements, 5 Addressable

note: The final rule has been modified to increase flexibility as to how protection is accomplished.

➢ ***Consider industry best practices.***

(Approximately 40+ outlined in the rule as guidance)

Final Security Rule- Key Concepts

Risk Analysis

- **"The most appropriate means of compliance for any covered entity can only be determined by that entity assessing its own risks and deciding upon the measures that would best mitigate those risks"**
- **Does not imply that organizations are given complete discretion to make their own rules- *Addressable does not mean Optional***
- **Organizations determine their own technology choices to mitigate their risks**

Addressable Implementation Specifications

- Covered eternities must assess if an implementation specification is reasonable and appropriate based upon factors such as:
  - Risk analysis and mitigation strategy
  - Current security controls in place
  - Costs of implementation
- Key concept: "reasonable and appropriate"
- Cost is not meant to free covered entities from their security responsibilities

Addressable Implementation Specifications

- If the implementation specification is reasonable and appropriate, then implement it
- If the implementation specification is not reasonable and appropriate, then:
  - Document why it would not be reasonable and appropriate to implement the implementation specification and implement an equivalent alternative measure if reasonable and appropriate

    or
  - Do not implement and explain why in documentation

Other Concepts

- **Security standards extend to the members of a covered entity's workforce even if they work at home (transcriptionists)**
- **Security awareness and training is a critical activity, regardless of an organization's size**
- ***Evaluation*** **– Must have a periodic review of technical controls and procedures of the entity's security program**
- ***Documentation Retention*** **– Six years from the date of its creation or the date when it last was in effect, whichever is later**

Final Security Rule- Steps toward Compliance

Broad Areas of Compliance Readiness…

ctg HealthCare Solutions

Now

- Become familiar with the Security Rule and how it will affect your organization
- Put somebody in charge- appoint a CSO
- Determine PHI data flow, if not done already, and its existence in information systems
- Start examining security policies and procedures
- Start identifying existing security measures- administrative, physical, and technical

Broad Areas of Compliance Readiness…

ctg HealthCare Solutions

Before the end of the year

- Start conducting a Risk Analysis
  - Identify assets, threats, vulnerabilities, risk mitigation requirements
- Begin the development and prioritization of remediation projects
- Begin the development of training programs

Broad Areas of Compliance Readiness…

ctg HealthCare Solutions

In 2004

- Work toward Compliance
  - Create a Security Management Process
  - Begin acquiring needed technology and implementing system "fixes"
  - Train the workforce/couple with Privacy training
  - Create compliant policies, procedures, feedback loops- monitoring, audit trails, incident reporting processes, business continuity, etc.
  - Develop a process for ongoing risk assessment
- Keep informed on HIPAA Administrative Simplification Enforcement guidance from DHHS

Broad Areas of Compliance Readiness

ctg HealthCare Solutions

In 2005

- Check for compliance
  - Test security mechanisms
  - Make sure you have a running, annotated, up-to-date documentation file that supports your decision-making relative to each of the security standards
    - Addressable specifications should show your choices and why they constituted "due diligence" in your business environment

Enforcement

Enforcement

- For Security Rule Violations- no fines before 2005, but…
  - Like Privacy- complaint driven initially
  - Privacy violation: security incident cause?
  - More definition expected with Enforcement Rule
  - Law suits by private parties
  - Class-action suit if multiple patients
  - "60 Minutes Moment"- negative PR
  - Heightened Security Awareness @ Fed Level
  - Current Initiatives
  - HHS/CMS Outreach/ NIST/Industry Help
  - Future Privacy/Security

Heightened Security Awareness

- Federal Regs: Data Security
  - HIPAA
  - Gramm-Leach-Bliley
  - Sarbanes-Oxley (aftermath of Enron)
  - 21 CFR Part 11 (Pharmaceutical Industry)
  - National Security Telecommunications and Information Systems Security Policy (Number 11)
- Cybercrime Penalties
  - Amendments to the Federal Sentencing Guidelines have increased penalties for cybercrimes and terrorism involving the infrastructure- additional 10-15 years in prison
  - Proposed May 1; take effect November

Current Initiatives…

- **Rapid Bioterrorism Detection System**
  - **Public Health Research Institute receives grant from federal government for $500K to develop a rapid testing system for the detection of highly pathogenic organisms that have been identified by federal health officials as likely to be used in bioterrorist attacks**
  - **DHHS testing a data delivery system (ePocrates) for distributing bioterrorism reports to physicians' pdas; approx. 10,000 doctors taking part; will use Word documents attached to e-mails**
  - **National Preparedness and Response- HIMSS bioterrorism task force working on an IT network**

Current Initiatives

ctg HealthCare Solutions

- Generally Accepted Information Security Principles (GAISP)
  - Information Systems Security Association (ISSA) proposal to develop an overarching framework that will provide every organization, regardless of size, a common way to implement and manage infosec programs- operationally-oriented that will enable an organization to also meet other security and privacy mandates, which tend to be more goal-oriented

Outreach from HHS/CMS

- **$10M requested to be used for education and outreach for transactions, code sets, identifiers, and security to assist covered entities establish compliance (rather than penalizing violators)**
- **Consolidated Health Informatics Initiative (CHII): adopt uniform standards for the electronic exchange of clinical information (all federal agencies): HL7 messaging standards; NCPDP for ordering drugs from retail pharmacies; IEEE standards for medical devices; DICOM for digital imaging; LOINC for clinical laboratory results**

NIST Security Guidelines

ctg HealthCare Solutions

- FIPS 199 Guidelines for Federal Agencies to Determine the Level of Security Needed for Information Systems (May, 2003)
  - Categorize systems based on level of risk in the areas of confidentiality, integrity, and availability
  - Guidelines how different types of information- such as medical or legal- align with those categories
  - Minimum security measures for the information and the information systems in each category
- NIAP- Common Criteria
- NIST SP 800-12 Introduction to Computer Security (NIST Handbook)
- NIST SP 800-14 Generally Accepted Principles for Securing Information Technology Systems

http://niap.nist.gov

Industry Compliance Help…

- NCQA/JCAHO
  - Privacy certification for business associates, payers, providers, clearinghouses, IT vendors, financial institutions, practice management firms, third-party administrators, disease management associations, survey vendors
- URAC
  - Privacy and security certification
- EHNAC
- Best Practices
  - Various efforts around the country (IIT, etc.)

Industry Compliance Help

- **The Workgroup for Electronic Interchange (WEDI) and the Council for Affordable Quality Healthcare (CAQH):**

  healthcare coalitions for standardizing communications between health plans and the provider community, including physicians, billing services, vendors, and clearinghouses, all changes are in one place with implementation timelines and downloadable "best practices" guides:
  www.wedi.org/snip/caqhimptools

Future Privacy and Security?

- **Privacy: Federal law to become more stringent in line with State law- Federal pre-emption?**

- **Security: Additional media regulations- paper, oral companion rules to electronic final rule?**

In Conclusion…

- You and your corporation will judged by the courts and the enforcement agencies by whether you exercised "due diligence" toward HIPAA Security compliance requirements
- Security and Privacy are inextricably linked
  - Cannot have Privacy without Security
  - Privacy has already necessitated a degree of security implementation and compliance because of its safeguards requirements to protect PHI

Thank You

Questions?

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