Implementing the HIPAA Security Rule

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

Presentation Overview

ctg HealthCare Solutions

- Introduction
- Final Security Rule
  - Key Concepts
  - Benefits and Impacts
- Steps & Tools Toward Compliance
- Conclusions

ctg HealthCare Solutions

Introduction

John Parmigiani

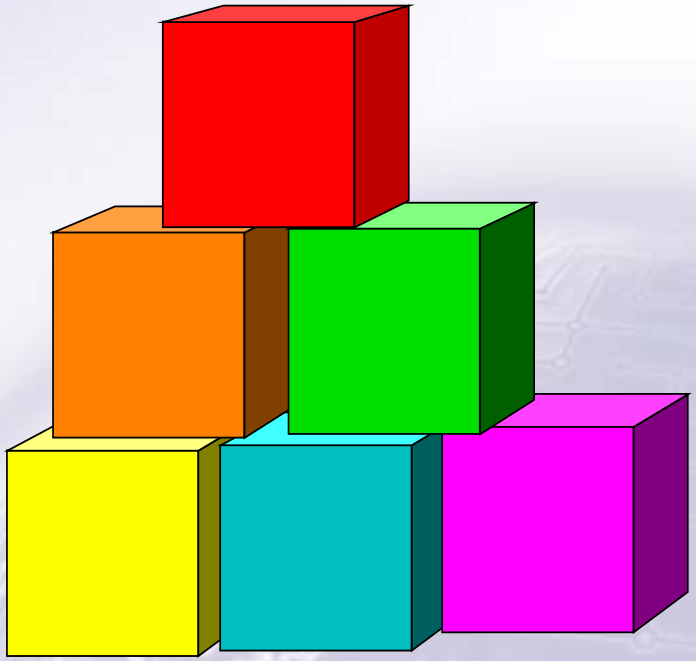
- **CTGHS National Director of HIPAA Compliance Services**
- **HCS Director of Compliance Programs**
- **HIPAA Security Standards Government Chair/ HIPAA Infrastructure Group**
- **Directed development and implementation of security initiatives for HCFA (now CMS)**
  - **Security architecture**
  - **Security 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**

ctg HealthCare Solutions

Final Security Rule

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

Security Axioms

ctg HealthCare Solutions

- **There is no such thing as 100% security**
- **Security is a business process**
- **Security is an investment, not an expense**
- **It is difficult to calculate the on return on investment for security**
- **Threats and risks are constantly changing**
- **Know your real risks**
- **Determine the probability and impact**
- **Prioritize your efforts**
- **Manage risks to an acceptable level**
- **Some security is better than no security**
- **Keep it simple and straightforward**
- **Security should be transparent to the user**
- **Security tools and products are like safety devices:**
    - Most of the time, you do not need them;
    - But those few times when you do need them…
- **Your overall security is only as good as your weakest link**

So…Security is Good Business

ctg HealthCare Solutions

- "Reasonable measures" need to be taken to protect confidential information (due diligence)
- A balanced security approach provides due diligence without impeding health care
- Good security can reduce liabilities- patient safety, fines, lawsuits, bad public relations
- Can have security by itself, but *Cannot have Privacy without Security!*

Consequences of Inadequate Security

ctg HealthCare Solutions

<u>Violation of patient privacy may result in</u>:

- **Civil Lawsuit**
  - ***Financial loss***
- **Criminal Penalties**
  - ***Fines and prison time***
- **Reputation**
  - ***Lack of confidence and trust***

Major threats: Dissatisfied Employees and Dissatisfied Patients

Or Worse…

ctg HealthCare Solutions

A breach in security could damage your organization's reputation and continued viability.

"There is a news crew from *60 Minutes* in the lobby. They want to speak to to you about an incident that violated a patient's privacy."

Security Rule Timeline

ctg HealthCare Solutions

- Originally posted to the Federal Register on August 12, 1998
- Rule was sent to the Office of Management and Budget (OMB) on January 13, 2003
- Published in *Federal Register* on February 20, 2003
- Compliance by April 21, 2005
- An extra year for small payers – Below $5 million: April 21, 2006

HIPAA Security Standards

ctg HealthCare Solutions

- Are based upon good business practices and
- Have these basic characteristics:
  - *Comprehensive*
  - *Flexible*
  - *Scalable*
  - *Technology Neutral*

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

ctg HealthCare Solutions

Old vs. New Terminology

- "Requirement" → "Standard"
- "Implementation Feature" → "Implementation Specification"

"Implementation Specification" → "Required" or "Addressable"

Comparison of Rules

ctg HealthCare Solutions

Old Proposed Rule –

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

New Final Rule –

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

Other Changes

ctg HealthCare Solutions

- **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**
- **Covers only <u>electronic</u> protected health information *(More limited than Privacy Rule)***
- **Requires a minimum level of documentation that must be periodically updated to reflect currently practices**

Terminologies Removed

ctg HealthCare Solutions

- **Formal** – Was used to convey documentation rather than word-of-mouth
- **Breaches** – Replaced by "security incident"
- **Open Networks** – Now up to the entity to determine when to apply encryption (addressable because there is not a simple solution to encrypting e-mails with patients)

Consider industry best practices.

Terminologies Clarified

ctg HealthCare Solutions

- **System** – "an interconnected set of information resources under the same direct management control that shares common functionality… includes hardware, software, information, data, applications, communications, and people."
- **Workstations** – "an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment."

HIPAA Security Standards

ctg HealthCare Solutions

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

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

ctg HealthCare Solutions

Key Concepts

Risk Analysis

ctg HealthCare Solutions

- "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
- Organizations determine their own technology choices to mitigate their risks

Addressable Implementation Specifications

ctg HealthCare Solutions

- 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

ctg HealthCare Solutions

- 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

ctg HealthCare Solutions

- Security standards extends 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 – Periodic review of technical controls and procedural review 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

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.

ctg HealthCare Solutions

Benefits & Impacts

Benefits

ctg HealthCare Solutions

- Establishes minimum baseline
- Encourages the use of EDI (increased confidence in the reliability and confidentiality)
- Promotes connectivity to provide availability of information
- Reduces the risks and potential cost of a security incident versus the increase in costs of additional security controls for compliance

Impacts – Responsibility

ctg HealthCare Solutions

- Responsibility must rest with one individual to ensure accountability
- "More than one individual may be given specific security responsibilities, especially within a large organization, but <u>a single individual must be designated</u> as having the overall final responsibility for the security of the entity's electronic protected health information."
- Aligns Security Rule with the Privacy Rule provisions concerning the Privacy Official

Other Impacts

ctg HealthCare Solutions

- Impacts will be dependent upon the size, complexity, and capabilities of the covered entity
- "Ensuring" protection does not mean providing protection, no matter how expensive.
- Balance between the information's identifiable risks and vulnerabilities, and the cost of various protective measures
- Enforcement not defined in the rule

ctg HealthCare Solutions

Steps & Tools Toward Compliance

Security Compliance Program Steps

ctg HealthCare Solutions

1. Appoint an official to oversee the program
2. Set standards of expected conduct
3. Establish training, education, and awareness program
4. Create a process for receiving and responding to reports of violation
5. Audit and monitor for compliance on an on-going basis
6. Take appropriate corrective actions

Serendipity Effect of Privacy Compliance

ctg HealthCare Solutions

- Complying with the Security Rule should be fairly easy if you have done the preliminary work for Privacy- PHI flow, risk assessments
- Implementation of "safeguards" to protect the privacy of PHI
- Balance through synchronization and symmetry

Next Steps

ctg HealthCare Solutions

- Assign responsibility to <u>one</u> person-CSO
- Conduct a risk analysis
- Deliver security training, education, and awareness in conjunction with privacy
- Develop/update policies, procedures, and documentation as needed
- Review and modify access and audit controls
- Establish security incident reporting and response procedures
- Make sure your business associates and vendors help enable your compliance efforts

Risk Analysis

ctg HealthCare Solutions

- What needs to be protected?
  (Assets – Hardware, software, data, information, knowledge workers/people)
- What are the possible threats?
  (Acts of nature, Acts of man)
- What are the vulnerabilities that can be exploited by the threats?
- What is the probability or likelihood of a threat exploiting a vulnerability?
- What is the impact to the organization?
- What controls are needed to mitigate impacts/ protect against threats

Information Security Policy

- The foundation for an Information Security Program
- Defines the expected state of security for the organization
- Defines the technical security controls for implementation
- Without policies, there is no plan for an organization to design and implement an effective security program
- Provides a basis for training

Audits

ctg HealthCare Solutions

- Data Owners periodically receive an access control list of who has access to their systems and what privileges they have
- Users are randomly selected for audit
- Audit data is provided to their managers
- Warning banners are displayed at logon to any system or network ("No expectation of privacy")
- Audit logs are stored on a separate system and only the Information Security Officer has access to the logs
- Audit trails generated and evaluated

Incident Reporting and Response

ctg HealthCare Solutions

- Can staff identify an unauthorized use of patient information?
- Do staff know how to report security incidents?
- Will staff report an incident?
- Is there one telephone number that staff can call to report any type of incident?
- Are there trained and experienced employees responsible for collecting and preserving evidence?
- Is the procedure enforced?

ctg HealthCare Solutions

Conclusions

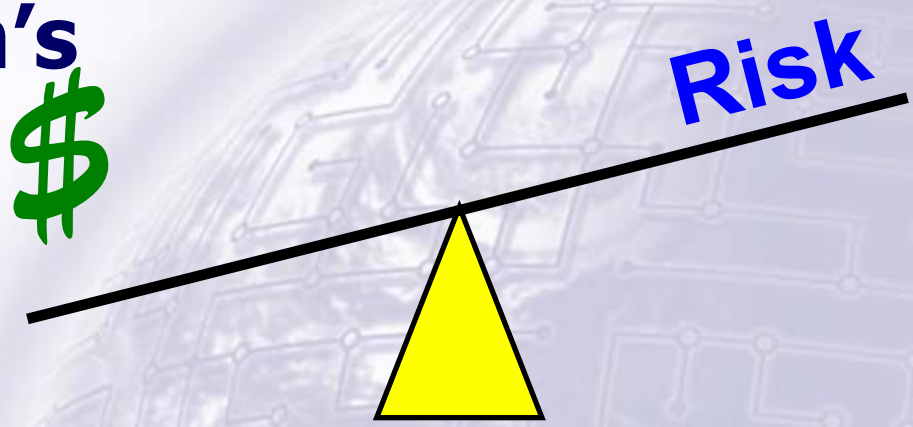
Reasonableness/Common Sense

ctg HealthCare Solutions

- 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

A Balanced Approach

- Cost of safeguards vs. the value of the information to protect
- Security should not impede care
- Security and Privacy are inextricably linked
- Your organization's risk aversion



Thank You

ctg HealthCare Solutions

Questions?

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