The Twelfth National

HIPAA Summit

Security Rule Compliance Update

John C. Parmigiani

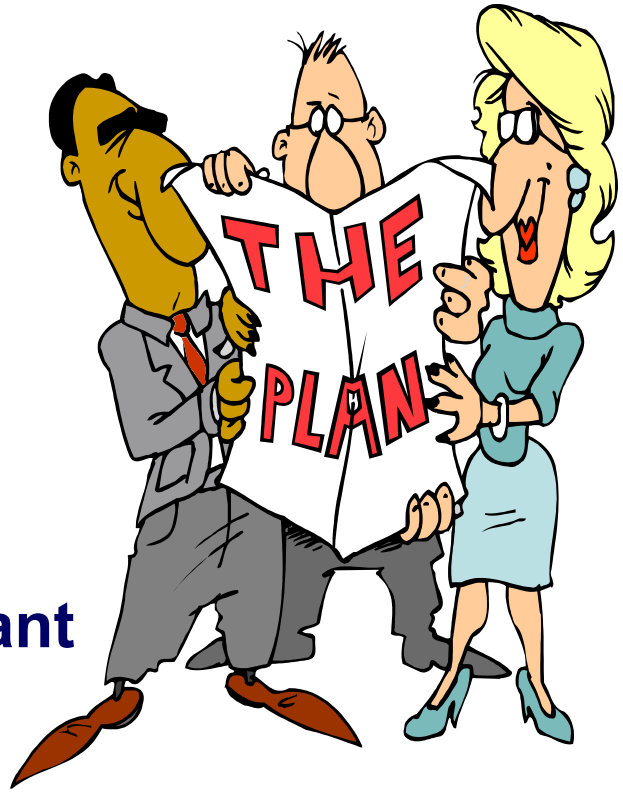
&

Gary G. Christoph, Ph.D.

April 11, 2006

Presentation Overview

- **The Healthcare Industry and HIPAA Security**
  - Where it should be
  - Where it is and why
- **What about Enforcement?**
- **Why the Security Rule is important**
  - Now
  - Future
- **Conclusions**



Healthcare & HIPAA Security

Where Healthcare should be

Almost one year since April 21, 2005 Security Compliance Date

+

Three years after Privacy Compliance Date (April 14, 2003)- included Security Safeguards

Covered Entities Should be Here!

- Have thoroughly read, discussed, and understood the requirements of the Security Rule (including “required” and “addressable”) and its implications to them for compliance
- Have obtained upper management buy-in
- Have appointed someone as the ISO, written a position description, provide high visibility and reporting responsibilities for the position, and communicated the name and contact information to the workforce
- Have set up a documentation book that chronicles your decisions and actions relative to Security Rule compliance
- Have determined PHI data flow and its existence in information systems
- Have created a complete inventory of information assets
  - Have a complete inventory of all hardware, software, in-house developed and vendor applications and their interfaces

Covered Entities Should be Here!

- Have reviewed existing information security policies, procedures, and plans for compliance with HIPAA security and created new or updated existing policies, procedures, forms, and plans as needed
- Have performed a Risk Analysis and developed a Risk Management Plan that delineates remediation efforts
  - Determined any new technologies required
  - Identified gaps in policies, procedures, processes
  - Implemented them
- Have maintained current documentation that supports decision-making relative to each of the security standards
  - Addressable specifications show the choices made and why those choices constituted “due diligence” for the business

Covered Entities Should be Here!

- Have verified that business associates are providing the same level of protection (safeguards and controls)
  - Have updated existing Business Associate Agreements that were signed for Privacy
  - Have engaged business associates and vendors in your compliance efforts
- Have established a formal information security training program
  - delivered the general training to the entire workforce;
  - developed and delivered focused training;
  - created methods for documentation and for various training delivery mechanisms;
  - established and trained staff on a security incident reporting process
- Have developed and implemented a process for creating user accounts that provide for access control (authentication and “need to know” for privileges)

Covered Entities Should be Here!

- Have formulated and implemented a “defense in depth” strategy to protect not only the network but also the internal electronic user interface from unauthorized access
  - Intrusion prevention/detection, malware protection, use of encryption for transmitting and storing ePHI, etc.
- Have implemented facility access controls to protect sensitive computing resources and data
- Have determined the audit capabilities of applications and systems as well as user activities and events that should trigger an entry into an audit log
- Have developed a Contingency/ Disaster Recovery Plan that provides for business continuity
  - Frequency, rotation, storage, and retention of back-ups
- Have established a review process for continued security compliance

Where Healthcare is

According to the latest Phoenix Health/HIMMS survey:

- ***55% of providers/ 72% of payers reportedly compliant***
- ***Many smaller providers haven't even started yet***
- ***Areas of concentration have been contingency planning (spurred by Katrina and Rita); emergency access procedures; risk analysis; and workstation use/management***

Why ?????

- *"lack of buy-in from senior leadership"*
- *"limited resources"*
- *lack of funding*
- *perception that Privacy/Security compliance creates obstacles to efficient healthcare delivery*
- *won't happen to us (despite the ever-increasing list of security breaches and corresponding losses in confidentiality, integrity, and availability to sensitive data in other industries)*
- *lax or no enforcement*

HIPAA Enforcement

HIPAA Privacy/Security Enforcement Stats

At the end of February, 2006:

- 18,300 complaints to OCR
  - second highest consistently is for “inappropriate safeguards”
  - approximately 500+/month
  - 72% closed with no fines imposed for noncompliance
  - 292 cases referred to DOJ for possible criminal prosecution (approx.10/month); one in the works (wrongfully using a unique health identifier with the intent to sell individually identifiable health information for personal gain)
  - controversial decision by DOJ in June, 2005 that criminal provisions do not apply to individuals only covered entities

HIPAA Privacy/Security Enforcement Stats

At the end of February, 2006:

- 51 security complaints to CMS; one closed

note: Security complaints have a smaller universe for their source – employees, ex-employees, contractors are more likely to detect and report than patients and beneficiaries

- *Only conviction to-date*: Gibson case in Seattle in November, 2004; considered a "toss-up" between HIPPA and identity theft prosecution

Statistics courtesy of Melamedia, LLC

Final Enforcement Rule

- Still encourages “voluntary compliance” as the most effective and quickest method
- Complaint-driven process
- Covered entity must have knowledge that a violation occurred to result in monetary penalties
- Cannot be cited for multiple violations related to one violation of a regulatory provision
- Stressed the importance of performing a risk analysis
- Must document decisions relative to adoption of addressable implementation standards

Other Drivers

- SOX; GLBA; 21 CFR Part 11; 42 CFR Part 2; CA 1386-like, PCI, etc. represent a certain "standard of care" to sensitive and personally-identifiable data
  - Going after certain directors, officers, and employees of these entities to hold them directly liable
- Penalties in 2005 for privacy/security violations; consumer awareness: ChoicePoint; LexisNexis; DSW; Time Warner; Bank of America; BJs; etc.
- Litigation; bad PR; accrediting bodies; competition from peers

Other Drivers

- E-commerce both nationally and internationally: business needs may be more powerful than regulatory enforcement
  - Governance and compliance may become performance metrics
  - Investment may be dependent on legal exposure to security data risks
- HIT initiatives – Congress and the President have used non-regulatory means to encourage the use of IT to improve health care delivery; bi-partisan; a number of bills proposed over the last year (most require HIPAA Privacy and Security Rules to be applicable)

E-Health Requirements

- Heavily dependent on Privacy and Security
  - Trusted relationships and communications
  - Real-time interoperability for effectiveness and efficiency
  - Accuracy (**integrity**) of ePHI to those systems and people with a “need to know” (**confidentiality**) and accessible when they need it (**availability**)
    - Authentication
    - Access controls to allowed data
    - Monitoring and recording access requests

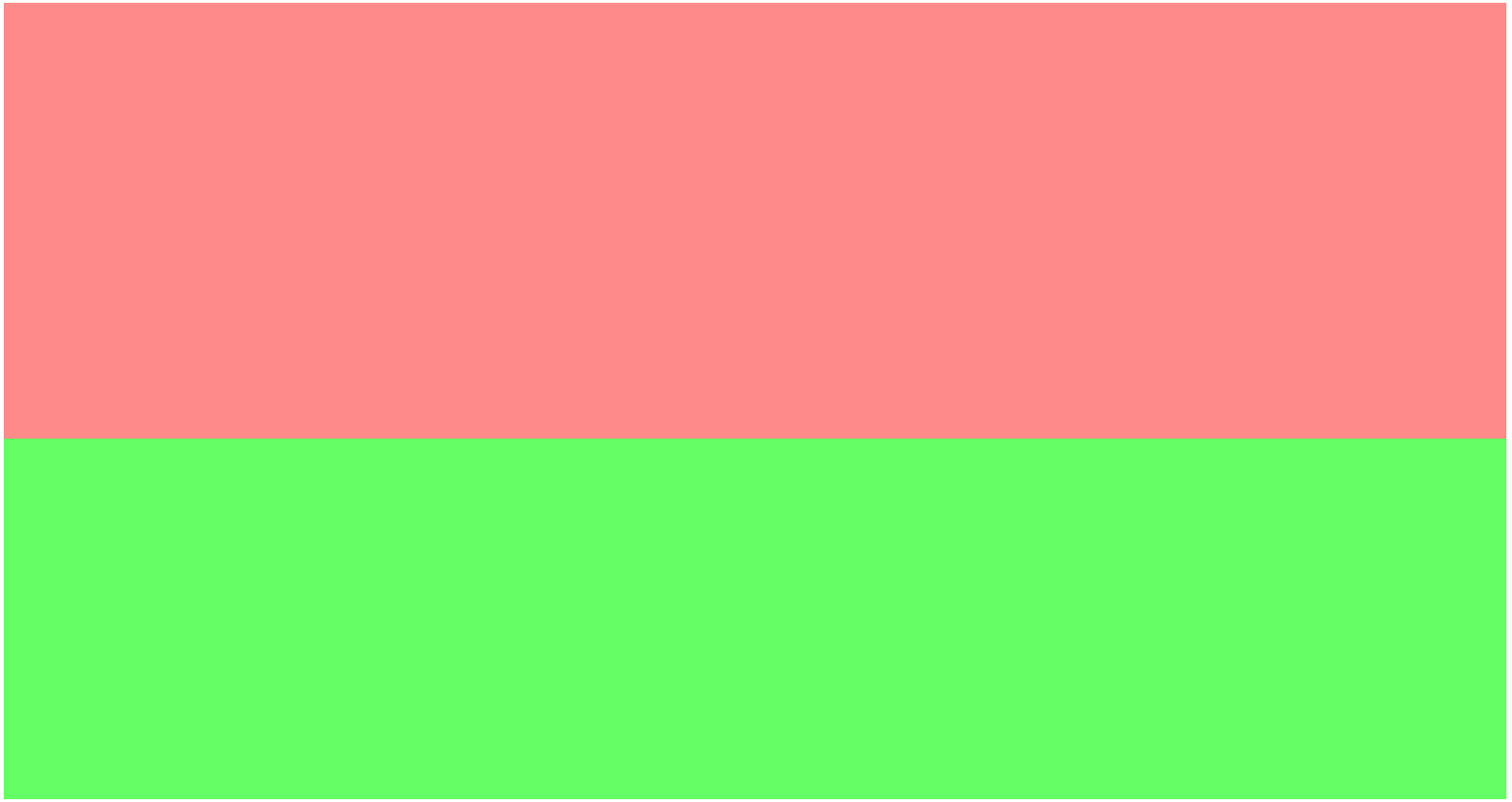
Importance of HIPAA Security

HIPAA Rules Shortcomings

- Scope Issue
  - Covered entities:
    - health plans, healthcare clearinghouses, health insurers, and healthcare providers that electronically pay or process medical claims, or that electronically transmit information associated with claims
  - Not covered are:
    - PHR and EHR organizations, online medical info providers, or RHIOs—any collector of private medical information that do not provide care nor are involved in insurance or payment
    - Investigative organizations that do not deal in payment or healthcare delivery
    - Researchers
    - State Health or Reporting Agencies that only collect PHI

HIPAA Rules Shortcomings

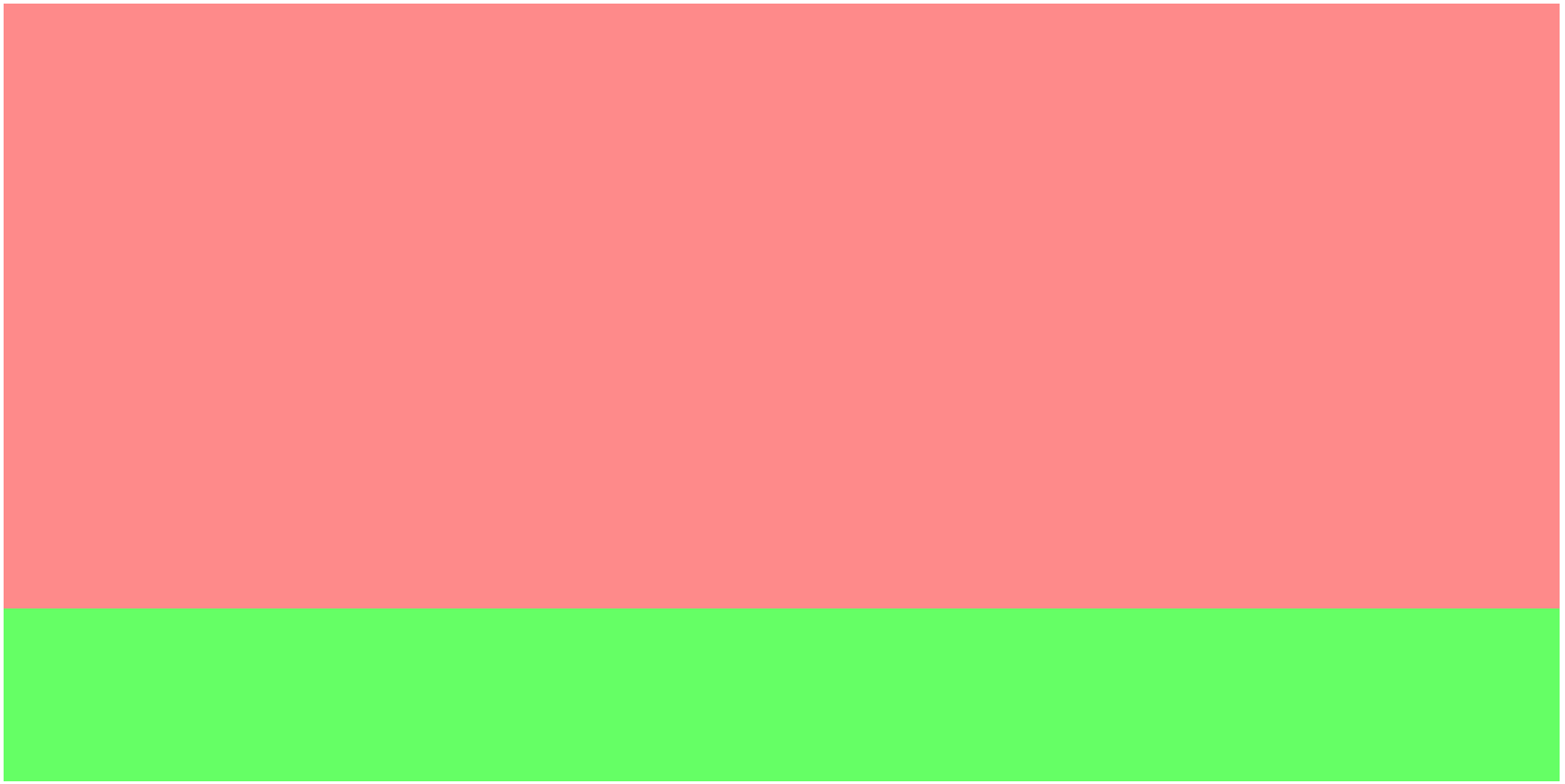
- Enforcement Issue:



HIPAA Rules Shortcomings

- 

State Security/Privacy Legislation



What is the real ROI of HIPAA Security/Privacy Controls

Conclusions/Actions Steps

Why Are We Here?

- Fundamentally, the driver for security/privacy controls is consumer trust in our business, not threat of enforcement
  - **Our business will suffer if our improper releases are made public**
  - **Security/Privacy will continue to be seen as a cost center, not a profit center**
- Thus our job is to:
  - **Educate our management**
  - **Secure systems and processes as best we can**
  - **Deal with inappropriate failures/disclosures of PHI**
  - **Develop business cases for security/privacy that include intangibles**
  - **Work with Public Relations to improve public perceptions of true risks**

Thank You!

Questions?

John C. Parmigiani
jcparmigiani@comcast.net
www.johnparmigiani.com

Gary G. Christoph, Ph.D.
gary.christoph@ncr.com