The Fourteenth National *HIPAA Summit*

HIPAA Security Rule Compliance Update

John C. Parmigiani
Gary G. Christoph, Ph.D.

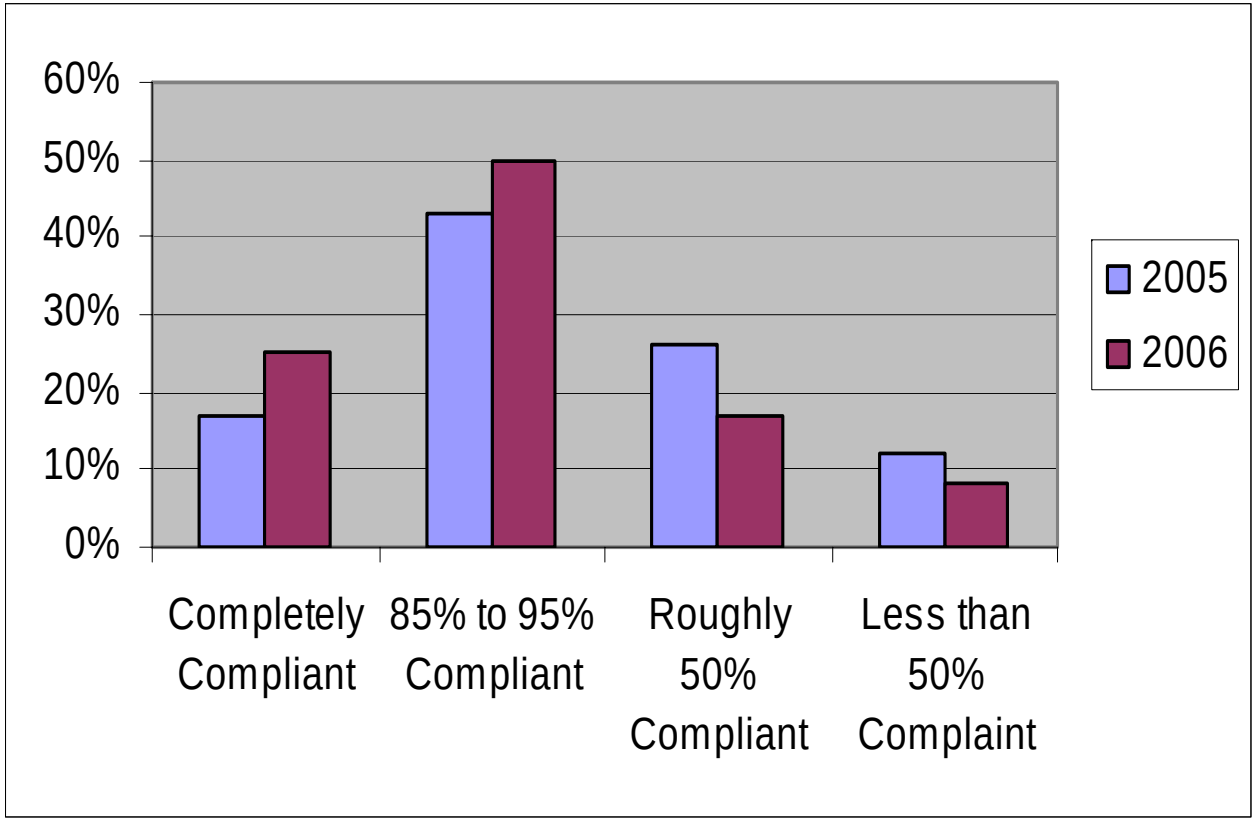
March 28, 2007

Presentation Overview

- Status of HIPAA Compliance
- Status of HIPAA Enforcement
- Reasons to Comply
- Discussion of Relevant Areas
- Conclusions
- Q&As

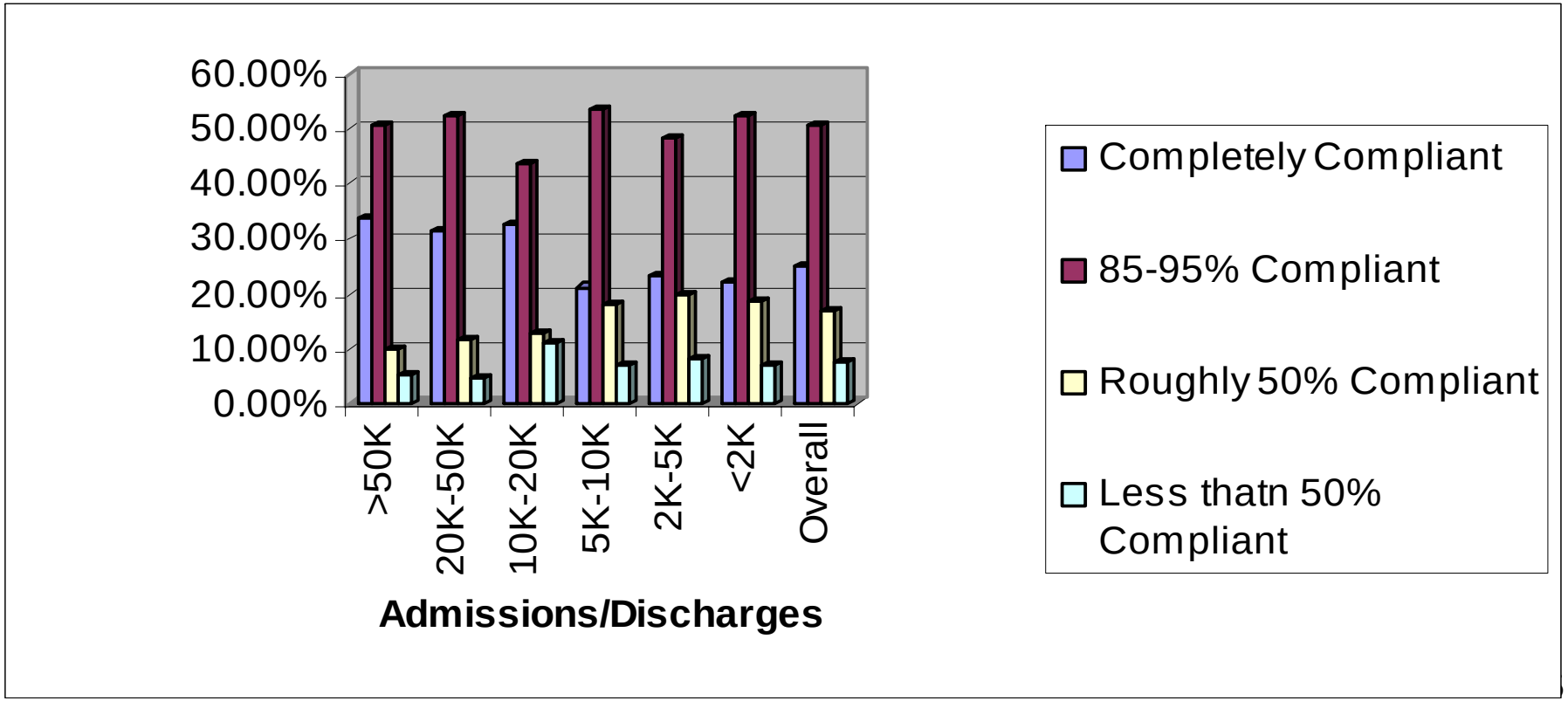
Status of HIPAA Compliance

AHIMA 2006 Survey

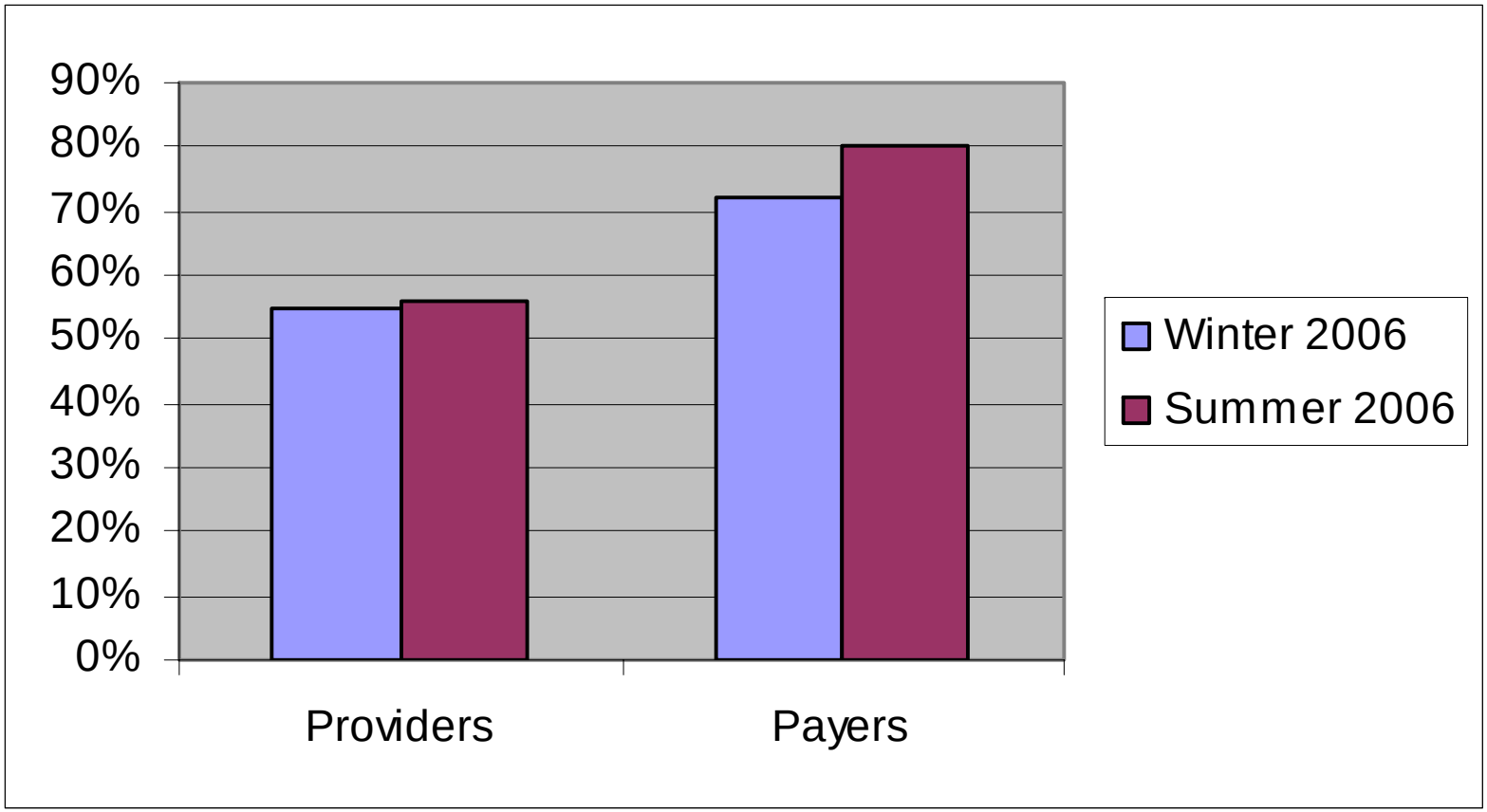


AHIMA 2006 Survey

- Surprisingly, larger facilities have only slightly higher compliance rates, smaller facilities have slightly lower compliance rates.



HIMSS-Phoenix Survey



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***
  - **Major HIPAA fear is of Bad PR rather than fines and/or imprisonment**

Status of HIPAA Enforcement

HIPAA Privacy Enforcement Stats

As of February 28, 2007:

- 25,662 Privacy complaints to OCR
  - second highest consistently is for **"lack of adequate safeguards for PHI" ~ security**
  - approximately 600/month
  - 77% closed with no fines imposed for noncompliance
  - 373 cases referred to DOJ for possible criminal prosecution (approx.10/month)—no criminal prosecutions reported

Statistics courtesy of Melamedia, LLC

HIPAA Privacy Enforcement Stats

- 4 convictions (neither from the OCR compliant system) – all brought by local federal prosecutors
- A “complaint-driven / voluntary compliance ” approach
  - *“One free violation” policy*
  - *Emphasis is on working with the non-compliant organization first, then, if corrective action is not attained, consider the imposition of civil monetary penalties (CMPs) – none to-date over a 4-year span*

HIPAA Security Enforcement Stats

As of January 31, 2007:

- 195* security complaints to CMS
  - 103 resolved/92 pending (53%)
  - reasons for complaints
    - Information access management
    - Security awareness and training
    - Access control counts
  - several (<10) cases referred to DOJ; no convictions

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

Statistics courtesy of Melamedia, LLC

Reasons to Comply

Regulatory Security Drivers…

- E-Health
  - EHR/PHR
  - E-Prescribing
  - RHIOs-data sharing
  - Patient/Physician/Provider portals
  - HIT initiatives and funding
    - Privacy and security are critical dimensions
    - “Trust” is essential to effective implementation

Regulatory Security Drivers…

- A Standard of Due Care
  - Payment Card Industry Data Security Standard
  - 21 CFR Part 11
  - 42 CFR Part 2
  - Gramm-Leach-Bliley
  - Sarbanes-Oxley (404)
  - Family Educational Rights and Privacy Act
  - Data Protection Acts (35 States and counting)

Regulatory Security Drivers

- A Standard of Due Care…
  - European Union Data Protection Standard
  - Japanese Data Protection Law
  - Canadian Personal Information Protection and Electronic Documents Act
  - Basel II
  - ….

➢ ***All have data security requirements common to HIPAA Security***

Other Emerging and Compelling Reasons…

New Enforcement Activities

- OIG's HIPAA Security Audit Initiative (#1 – March 5, 2007)
- GAO Report (2/05/07)
- New False Claims Act Guidelines (effective 1/1/07)
- New eDiscovery Rules (effective 12/1/06)

Other Emerging and Compelling Reasons…

On the Horizon

- Identity Management and Federated IdM for information sharing and in AMCs
- Security Breach Notification Laws (35 States) -> Federal Regulation ? (preemptive)
- ONCHIT and AHRQ activities regarding EHRs, EMRs, and Health Information Exchange

Other Emerging and Compelling Reasons…

Good Business

- Identity Theft/Medical Identity Theft (50% increase over the last three years- 15 million in 2006)
  - Cyber Insurance – one company will pay a healthcare organization's (hospitals, physician groups, healthcare software providers, claims processors, image delivery systems, LTC facilities, and MCOs) expenses to cover regulatory mandated notifications that a security breach has occurred as well as fines, fees, and penalties arising from privacy or consumer protection errors

Other Emerging and Compelling Reasons

…Good Business

- Security concerns spur emphasis on risk management and process improvement – shift is away from just compliance to running the business more efficiently and effectively
- Examples where HIPAA compliance helped
  - Illinois decision (1/19/07) that because there was documented proof that an employee who had improperly disclosed patient information had been trained (more than once) and there was existing organizational policy concerning patient confidentiality the hospital could not be sued.

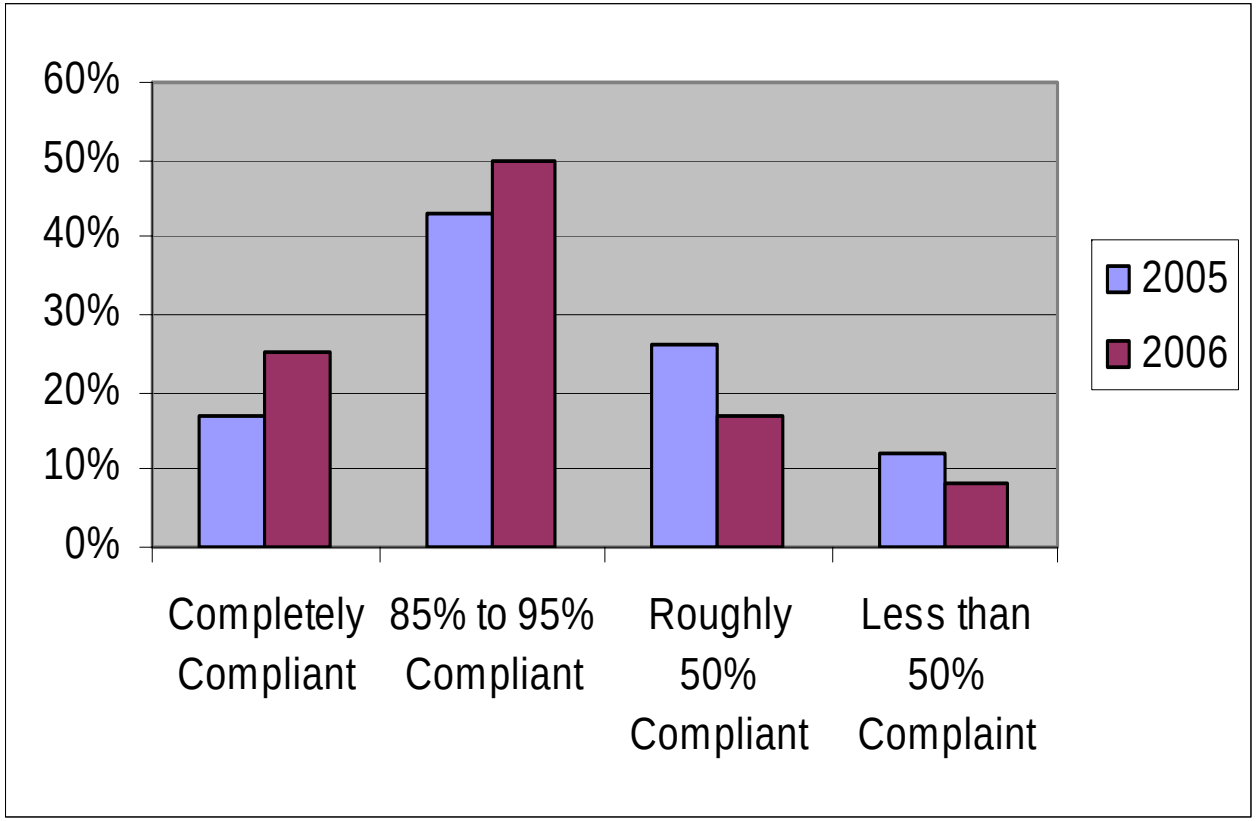
HIPAA Security Compliance

Gary G. Christoph, PhD

Teradata Government Systems

March 30, 2007

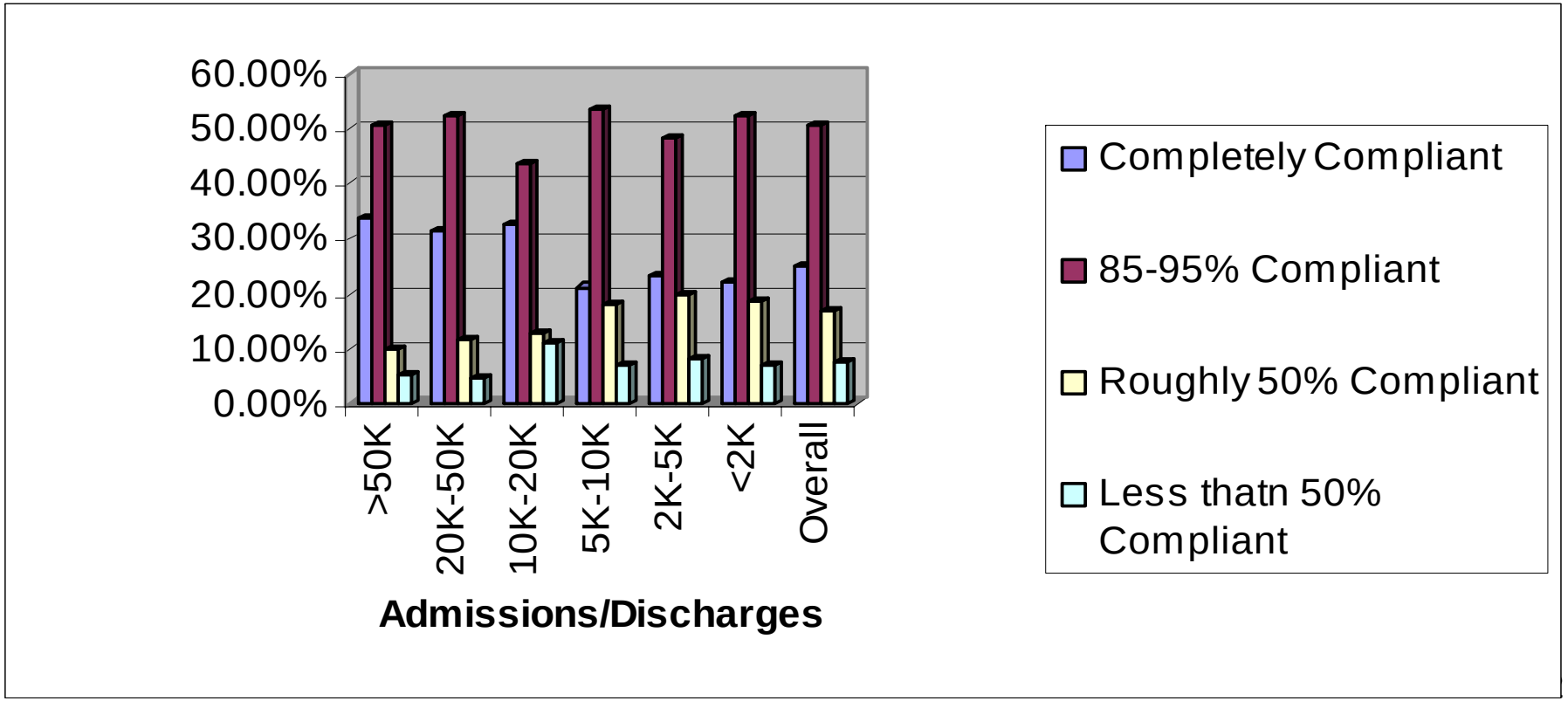
AHIMA 2006 Survey



N = 1,117 Privacy Professionals in hospitals or integrated delivery systems

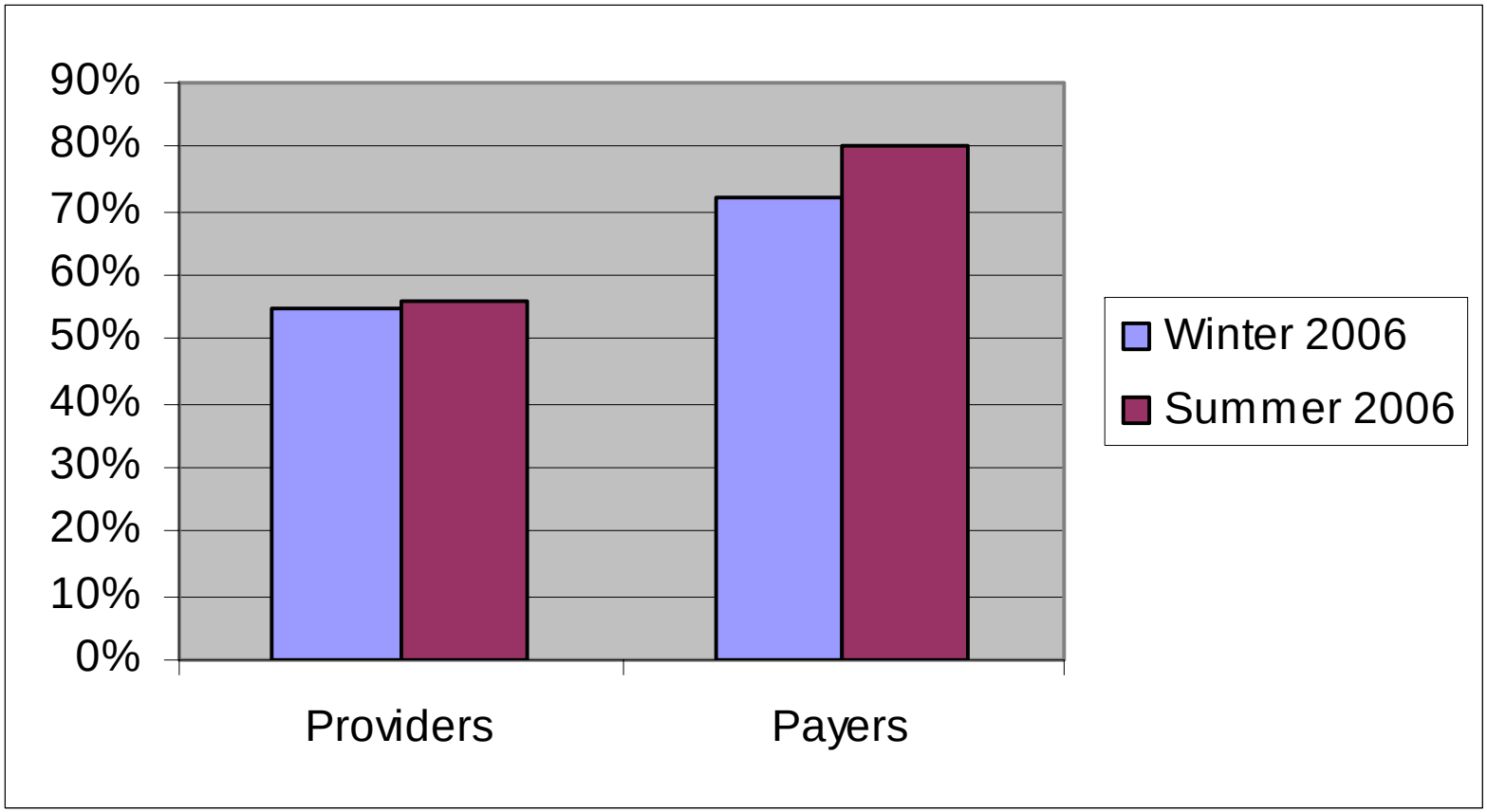
AHIMA 2006 Survey

- Surprisingly, larger facilities have only slightly higher compliance rates, smaller facilities have slightly lower compliance rates.



HIMSS-Phoenix Survey

Security Rule Compliance



N = 220 (81% Provider Organizations, 19% Payers)

Progress?

- Depending which survey you believe, HIPAA Security Compliance is slightly up from a year ago.
- The disarming fact is that the self-reported numbers are still low, only about 25% fully compliant, with about 50% mostly there.
- Survey numbers are small
- Enforcement is still light to absent, with the emphasis on assisting those complained-about providers with becoming compliant.
- The only “Good News”: Security Compliance is ahead of Privacy Compliance

HIPAA Security Compliance

- Awareness of Security Issues ***has*** increased
  - Reasons:
    - **Greater public awareness of identity theft**
    - **Everyone gets Privacy compliance flyers**
    - **Sensitivity to being reported in the news**
    - **Security rule is easier to comply with than privacy**
    - **As providers get into it, it becomes easier to confront problems**

Current Problems?

- Evolution of technology is fast
  - Evolution of policy and regulation is slow
- Trust model evolution
  - For greater interchange of data, there is a movement to the edge--centralized trust models do not work well
- Ownership of data is a privacy policy issue, not a security issue
- Government cannot alone change how healthcare is delivered
  - Need changes in how healthcare is delivered
  - “Piecework model” at the beginning of its evolution
  - What are the drivers for change?

The Debate on EMRs

- EMRs becoming more talked about
- Exchange of PHI being discussed, prototyped, implemented by RHIOs
- AHRQ/NGA Survey of 34 States and Territories to examine “barriers” to HIE
- NPI compliance due this May; a critical piece to Health Information Exchange in implementation of EMRs is accurate authentication

AHRQ/NGA “Barriers” Study

- Most “States” currently have only about 9%-20% “acceptance” of EMRs
- State-wide RHIOs are forming, but most lack a viable business model
- Confusion about HIPAA privacy a perceived barrier
- State laws still largely lodged in “paper world”
- Practice habits a barrier: providers are *uncomfortable* with electronic interchange; but providers are *more comfortable* with paper
- Technical security solutions beginning to be addressed, but likely requires legislative changes

Health Information Exchange

- RHIOs now mostly local
  - **BAAs multiply exponentially as the number of participating entities grows**
- RHIOs are new “Information Brokers”
- RHIOs generally not legally recognized
- Certain identification of patients a recognized difficulty
  - **What happens if test results for patient A get put into patient B’s EMR?**
- States just beginning to recognize that inter-state HIE raises potential issues

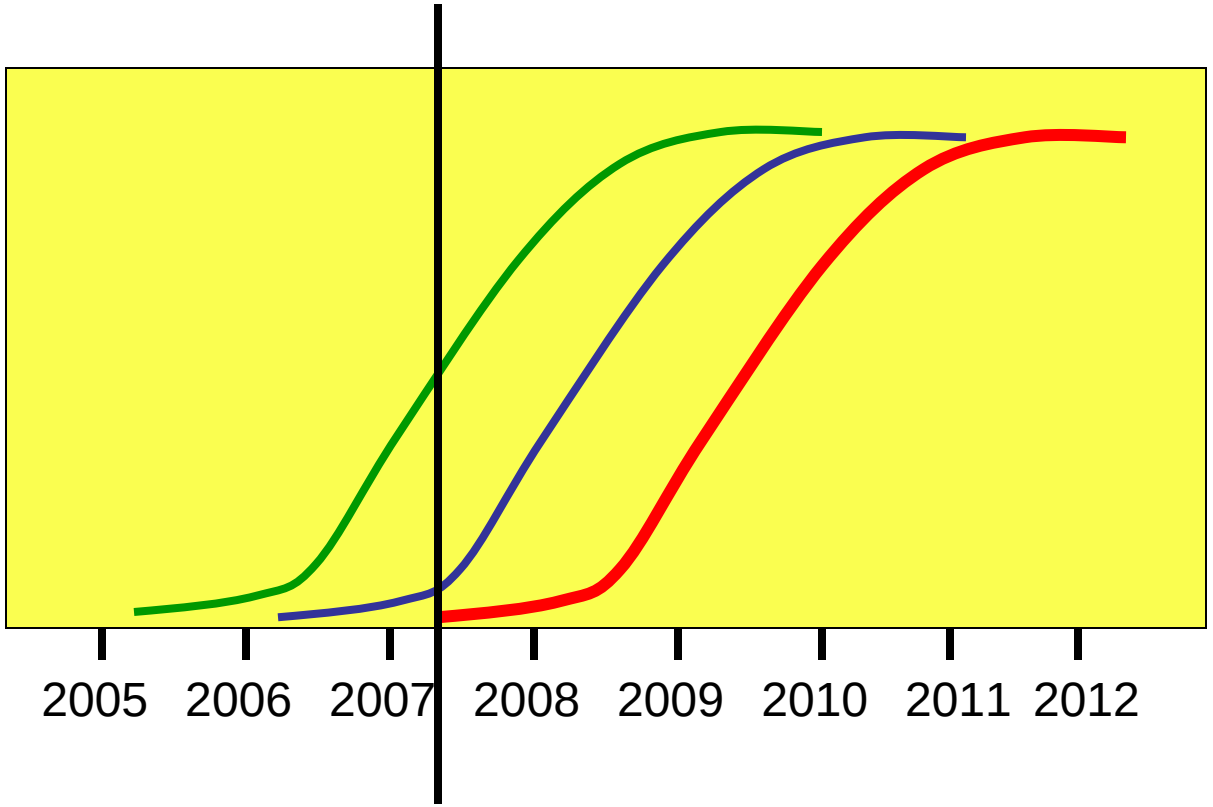
Debate: Federated vs Centralized

- Federated model
  - PHI stored at each provider
  - Central “finder” points to various holders of records for each patient.
  - Trust in privacy/security policy strength of *each* data holder
  - Accurate identification of data contributors and users problematical
- Centralized model
  - PHI stored centrally, contributed by providers, patients
  - Trust in strength of privacy/security policy protections at central holder
  - Accurate identification of contributors and users largely a political problem

Conclusions

Healthcare Transformation?

- Where is the tipping point?



Quotes from HIPAA XIV

- Rob Kolodner:

  "Security, Privacy, and Confidentiality are foundational to the transformation of the healthcare environment."

- Peter Swire:

  "Inevitable things eventually happen."

- Jon White:

  "Never doubt that a small group of thoughtful committed people can change the world" – Margaret Mead

- Randy Cohen:

  "Three can keep a secret if two of them are dead" – Ben Franklin

What Have We Said

- HIPAA is just common sense
- Many excellent tools to secure your practices exist (e.g., disk encryptors, AD, VPNs, FWs), but we will *never* have perfect security
- Main HIPAA compliance driver is largely fear of public reaction to PHI disclosure
- Good security is mandated by many laws besides HIPAA (e.g., SOX, GLBA, CA SB1386)
- ROI of good security practices can be huge, when you consider that disclosure can mean loss of customers, lowered stock price, loss of consumer confidence in your organization, death of your organization
- Little fear of fines or sanctions by HHS or CMS

Thank You, You small group of committed people !

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

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