The Thirteenth National

HIPAA Summit

HIPAA Security Rule Compliance Update

John C. Parmigiani
Uday Ali Pabrai, CISSP, CSCS
Gary G. Christoph, Ph.D.

September 27, 2006

The Presenters

- **John C. Parmigiani**, **President**

  John C. Parmigiani & Associates, LLC

- **Uday Ali Pabrai**, **CEO & Co-founder**

  HIPAA Academy/ecfirst.com

- **Gary G. Christoph**, **Ph.D, Chief Informatics Officer**

  Teradata Government Systems, Inc.

Presentation Overview

- HIPAA and Healthcare
  - Where and Why
  - Enforcement Stats
- Comply with HIPAA Security
  - Directly or Indirectly
- Key Areas
- Relevant Guidance
- Conclusions
- Q&As

HIPAA & Healthcare

Where Healthcare is

According to the latest Phoenix Health/HIMSS 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 Privacy Enforcement Stats

As of July 31, 2006:

- 21,434 Privacy complaints to OCR
  - second highest consistently is for **“inappropriate safeguards“ ~ security**
  - approximately 600/month
  - 75% closed with no fines imposed for noncompliance
  - 337 cases referred to DOJ for possible criminal prosecution (approx.10/month)
  - 2 convictions (neither from the OCR compliant system)
- As of September 1, 2006, one new indictment!

Statistics courtesy of Melamedia, LLC

HIPAA Security Enforcement Stats

As of August 15, 2006:

- 127* security complaints to CMS
  - 53 resolved/74 pending
  - 2 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

HIPAA/??? Compliance

Security Drivers

- E-Health
  - EHR
  - E-Prescribing
  - RHIOs-data sharing
  - Patient/Physician/Provider portals
  - HIT initiatives and funding
- Major HIPAA fear is of Bad PR rather than fines and/or imprisonment
- A Standard of Care

Don’t Want to Comply with HIPAA, but

- Do you use credit cards in your healthcare organization? ***PCI Data Security Standard***
- Do you have medical devices? ***21 CFR Part 11***
- Do you have patients with alcohol or substance abuse? ***42 CFR Part 2***
- Do you send and receive financial data to banks? ***GLBA***
- Are you a for-profit organization? ***SOX***

Don’t Want to Comply with HIPAA, but

- Are you an Academic Medical Center? ***FERPA***
- Do you do business in California or 35 (and counting) other states? ***CA SB 1386, etc.***
- Do you do any international business?

EU Data Protection Directive

Japanese Data Protection Law

Canadian PIPEDA

Basel II

……….

Common Security Requirements

- Protect sensitive data at rest and in transit
- Restrict data access on need-to-know basis
- Authentication/Access Controls/Audit Controls
- Business continuity
- Network protection
- Security management process
  - Administrative, Physical, Technical safeguard areas

Key Security Areas

Typical Security Remediation Initiatives

- **Enterprise Security Priorities**
  - Deploy Firewall Solutions, IDS/IPS
  - Secure Facilities & Server Systems
  - Deploy Device & Media Control Solutions
  - Implement Identity Management Systems
    - Single Sign-On (SSO) solutions
  - Deploy Access Control Solutions
  - Implement Auto-logoff Capabilities
  - Deploy Integrity Controls and Encryption
  - Activate Auditing Capabilities
  - Test Contingency Plans

Identity Management

Authentication factors may be one or more of the following:

- Something you know (knowledge)
- Something you have (possession)
- Something you are (person)

Strong authentication solutions include:

- Tokens
- Smart cards
- Biometrics

Identity Management Best Practices

- Use multi-factor authentication
- Track method from issuance to deactivation
- Manage emergency access procedures
- Ensure logging

Wireless Challenges

- **Lack of user authentication**
- **Weak encryption**
- **Poor network management**
- **Vulnerable to attacks:**
  - Man-in-the-middle
  - Rogue access points
  - Session hijacking
  - DoS

Wireless Best Practices

- **Conduct risk analysis**
- **Develop security policies**
  - Wireless
    - Mobile devices
  - Encryption
- **Remediation: Design infrastructure**
  - Firewall
  - IDS
  - Wired network

Evaluate & Audit

- **Establish Processes for:**
  - Risk Management
  - Audit

- **Deliverables:**
  - Ensure Compliance with legislation(s) and standard(s) as required
  - “Close and Lock” all Security Gaps

The Importance of Audits

- Audit provide insight into vulnerabilities of an organization
- Audit on a regular basis
- Audits conducted must be thorough and comprehensive
- Strong audit trails help the entity ensure the CIA of sensitive information and other vital assets

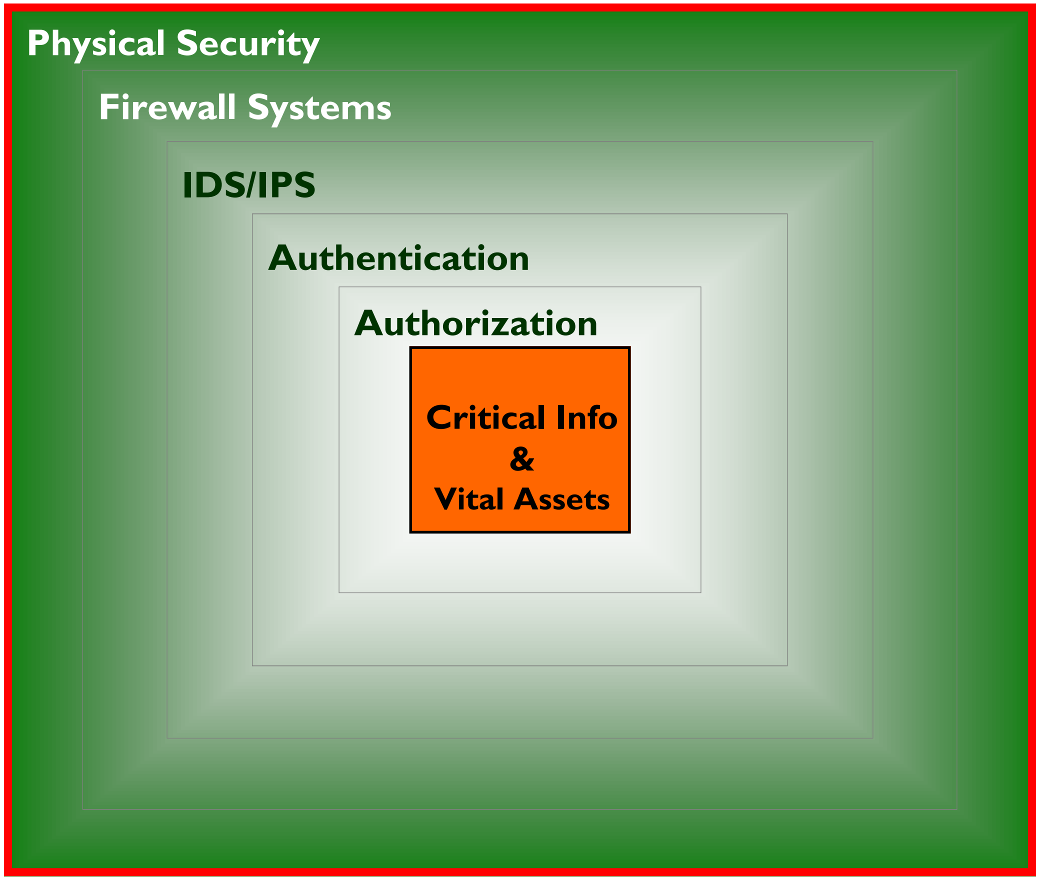
Key to responding to Security incident/complaint

Standards & Regulatory Compliance

Seriously influence security architecture priorities:

- HIPAA
- ISO 17799:2005
- FISMA
- Sarbanes-Oxley
- GLB
- California Privacy/Security Laws

Defense In-Depth



Relevant Guidance

HIPAA Administrative Simplification Compliance Deadlines

Date	Deadline
October 15, 2002	Deadline to submit a compliance extension form for Electronic Health Care Transactions and Code Sets.
October 16, 2002	Electronic Health Care Transactions and Code Sets - all covered entities except those who filed for an extension and are not a small health plan.
April 14, 2003	Privacy - all covered entities except small health plans.
April 16, 2003	Electronic Health Care Transactions and Code Sets - all covered entities must have started software and systems testing.
October 16, 2003	Electronic Health Care Transactions and Code Sets - all covered entities who filed for an extension and small health plans.
October 16, 2003	Medicare will only accept paper claims under limited circumstances.
April 14, 2004	Privacy - small health plans.
July 30, 2004	Employer Identifier Standard - all covered entities except small health plans.
April 20, 2005	Security Standards - all covered entities except small health plans.
August 1, 2005	Employer Identifier Standard - small health plans.
April 20, 2006	Security Standards – small health plans.
May 23, 2007	National Provider Identifier - all covered entities except small health plans
May 23, 2008	National Provider Identifier - small health plans

Useful HIPAA Security Guidance

- www.cms.gov/hipaa CMS guidance
- www.hhs.gov/ocr/hipaa HHS guidance
- www.ahima.org/emerging_issues AHIMA resource list
- csrc.nist.gov/publications/nistpubs/800-66/SP800-66.pdf NIST Special Publication (SP) 800-66
- http://www.hipaadvisory.com/regs/securityoverview.htm Phoenix Health Systems site
- http://www.sans.org/reading_room/whitepapers/hipaa/ SANS Security Organization
- www.acha.org/info_resources/hipaa_links.cfm American College Health Association

Conclusions

Value of Surveys?

- Self-reported data is suspect
- Small sample sizes
- Motivation to not respond if not compliant

Conclusion:

- We have few good numbers to gauge our progress

What are ***your*** motivators for HIPAA compliance?

- HIPAA requirements?
- GLBA requirements?
- SOX requirements?
- CA SB 1386 (or State copy-cat) requirements?

Data Breaches are Inevitable

Entity*	Type of Breach	# of Individuals Affected
Department of Justice	Stolen laptop (5/7/05)	80,000
MN Dept of Revenue	Missing data tape backup package	50,400
U.S. Navy	Files on civilian web site	30,000
Equifax	Stolen company laptop	2,500
American Red Cross	Dishonest employee (5/24/06)	1,000,000
Kent State University	Stolen laptop (6/17/05) Stolen computers (9/10/05)	1,400 100,000
CitiFinancial	Lost backup tape (6/6/05)	3,900,000
Designer Shoe Warehouse	Hacking (3/8/05) Hacking (4/18/05)	100,000 1,300,000

Breaches are almost always caused by human error.

**Source: Estimates based on various news media reports*

Data Breaches Are Common!

Over 20% of the US population has had their personal information lost or stolen already this year

Recent Data Breach Costs Are *Astronomical!*

ChoicePoint

- Legal Fines = **$15 Million**
- Contacting consumers and credit monitoring = **$2 Million**
- Other
  - Market capitalization loss = **$720 Million**
  - Direct breach charges, excluding fines = **$11.5 Million**

TOTAL: over **$?? Million**

+

+

Veterans Affairs Department

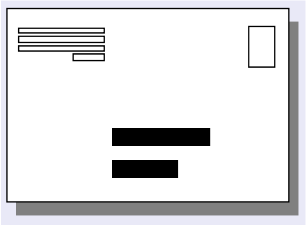
- Notification letters to 17.5 million veterans = **$7 M**
- Legal Fines
  - Lawsuit filed requesting $1,000 per victim = **$26.5 Billion**
- Credit Monitoring **(N/A)**
- Call Center = **$200,000 per day (\$10+Million)**

TOTAL: over **$?? Million**

**Source: Estimates based on various news media reports*

Remediation is More Expensive than ***Prevention***

Notification Letter



$1.50-2.00 per individual

Call Center

$10 to $31 per call

Legal Fees

$1,000+ per case

Fines / Penalties

$1000-$250,000
per incident

Credit monitoring

$60 per person

Loss of consumer confidence

Priceless

**Source: Estimates based on various news media reports*

What Have We Said

- HIPAA is just common sense
- Many excellent tools to secure your practices exist
- 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 !

Questions?

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

Ali Pabrai, CISSP, CSCS
uday.pabrai@ecfirst.com

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