

# HIPAA Security Too Little Too Late

April 6-8, 2005

10<sup>th</sup> National HIPAA Summit

**iTM**<sub>1</sub>

# Most Insurers, Providers Unprepared for HIPAA Security Deadline

- ***Modern Physician***—February 2004 January survey of 400 insurers and providers
  - Only 30% of insurers and 18% of providers are in compliance with HIPAA security rules
  - 80% of payers and 74% of providers said they expect to meet security requirements by the deadline
  - Last June 91% of payers and 87% of providers said they expected to meet the deadline
- ***U.S. Healthcare Industry HIPAA Compliance Survey Results, Winter 2005***
  - 70% of insurers and 73% of providers are in compliance with the HIPAA transactions and code sets rule, up from 62% and 65% six months ago, respectively.
  - Contradiction??? The survey also found that 65% of insurers and 48% of providers are taking part in the CMS contingency plan for HIPAA TCS compliance.
  - 90% of insurers and 78% of providers are compliant with the HIPAA privacy rule **nearly two years** after the April 2003 deadline.
  - 56% of insurers and 73% of providers said their organizations had experienced **one or more privacy breaches in the past six months**

**Healthcare's Track Record of Too Little, Too Late!!!**

# Background

- Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- The law gave Congress until August 21, 1999, to pass comprehensive health privacy legislation.
- November 1999, HHS published proposed regulations to guarantee patients new rights and protections against the misuse or disclosure of their health records
- Transactional and Privacy Rules already in effect
- **Security Rules which will take effect on April 21, 2005** covering 3 areas
  - Each with “Required” and “Addressable” Topics

# Administrative Requirements

- Documented formal practices
- Security measures to protect data
- Policies / procedures regarding conduct of personnel vis-à-vis protecting PHI
- Formal employee termination procedures
- Security incident procedures
- Security training.

# Physical Requirements

- Protection of physical computer systems
- Network and topology safeguards
- Environmental hazards & disasters
- Physical intrusion
- Considerations
  - Placement of computer screens preventing unauthorized viewing
  - Placement of fax machines and printers that may contain PHI.
  - Locks, keys, and administrative measures that control access to computer systems and facilities.

# Technical Requirements

- Services and mechanisms relating to PHI stored on the computer network.
- Security mechanisms relating to PHI transmitted over a communications network such as the internet, VPN, frame relay, private line, or other network.
- Formalized policy of reporting Security Breach

# Addressable HIPAA Security Categories

- Workforce authorization, modification, and termination
- Security training, communication, and culture change
- System management—strong passwords, audit logs
- Contingency planning, testing, data backup, and criticality analysis
- Data protection controls—encryption, auto logoff, data integrity

# What Does It Mean

*Whether in paper or electronic form, medical record information can no longer be left unguarded, where a casual observer, a snoop, or a thief can have access to it—This includes INTERNAL staff!*

## Trusted Systems ,Trusted Employees and Trusting Patients

**Kaiser Permanente** is alerting 140 patients in Northern California that a disgruntled former employee posted private information about them on her blog, the *San Jose Mercury News* reports. The information includes medical record numbers, patient names and information about some routine lab tests, but not the test results.

Kaiser in **January learned of the breach** from the federal **Office of Civil Rights** and has been investigating the issue since then, said Kaiser spokesperson Matthew Schiffgens. However, Schiffgens said Kaiser on **Wednesday** asked the Internet service provider hosting the blog to remove the data, the *Mercury News* reports.

The former employee, said that the company posted the patient information on an unsecured Web site and that Kaiser took it down only after she pointed it out, the *Mercury News* reports. She said she reposted the information to another site to illustrate how easy it was for someone to access the information, which she said had been on the Internet for a year. She said she also filed a complaint with the federal Office of Civil Rights.

Schiffgens said Kaiser has been unable to confirm the woman's claims that it posted private patient data, but he said the woman still breached her obligation to protect member confidentiality by posting the information herself. Schiffgens said Kaiser might take legal action against the woman, the *Mercury News* reports. **Under HIPAA rules, she could face fines of up to \$250,000 and 10 years in prison for unlawfully disclosing patient data** (Feder Ostrov, *San Jose Mercury News*, 3/11).

# Hitting Close To Home



February 8, 2005

007688

WAYNE F MACKERT  
6011 152ND AVE SE  
BELLEVUE WA 98006

This letter is to inform you that Principal Life Insurance Company's disease management program provider, American Healthways, experienced the theft of a computer containing data from The Principal. The theft occurred Saturday, January 29, when an unauthorized person accessed secured office space in American Healthways' headquarters and stole a computer from an employee's desktop. ***Please read this letter carefully and in full, as it contains information important to you.***

## CMS Issues New HIPAA Security Guidance

- CMS guidance ... covered entities not required to certify compliance with the rule's provisions
- Must perform regular technology and non-technical security evaluations
- Evaluations can internal or by an external organization that provides evaluations or certification services
- Certification by an outside organization does not prevent an ultimate HIPAA security finding

*Health Data Management, August 2004*

# Internal Threats Loom Large

- Oct. 2004 The Office for Civil Rights has received over 8,000 complaints alleging violations of the privacy rule in some manner

## A Trusted System defeated by Untrustworthy Employee

- The Employee had direct contact with patients, and one of them had come to Seattle from outside of the State of Washington in order to receive treatment from the Seattle Cancer Care Alliance, where the Employee worked. The patient found out that someone had stolen his identity, specifically his name, Social Security number, and date of birth, and used that information to get credit cards in his name.
- This clearly was unlawful identity theft, but it was also a violation of HIPAA's criminal provisions since the information had been collected from him because he was a patient....this is the first case prosecuted by a U.S. Attorney's Office under the HIPAA criminal statute.

**A Harbinger of things to come regarding Security Violations!!!!**

# A Privacy Violation Is Likely A Security Violation Too!

- Due to the possibility of disclosure of information over computer networks and the sensitive nature of some medical conditions and treatments, HIPAA-related cases have the potential to become high-stakes litigation with multiple plaintiffs who seek compensation plus punitive damages.
- ***"The creative way to use HIPAA is arguing that HIPAA sets a federal standard of care for the privacy and security of health information,"*** Leigh-Ann M. (Patterson) Durant, a litigation and health care law partner at Nixon Peabody LLP

# Growing Insider Threat

According to a recent U.S. Secret Service and Carnegie Mellon CERT/CC Survey

- 23 incidents by 26 insiders in the banking and finance sector between 1996 and 2002.
- 15 involved fraud, four the theft of intellectual property and four sabotage.

Conclusion: *"Insiders pose a substantial threat by virtue of their knowledge of and access to their employers' systems and/or databases, and their ability to bypass existing physical and electronic security measures through legitimate means."*

August 31, 2004 - Source: SearchSecurity.com

## Case Study: Pacific Medical Centers Security Assessment & Accreditation

- Pacific Medical Centers is a Hybrid healthcare organization
  - 6 Clinics & Headquarters Campus
  - 110+ Physicians
  - 600 Staff
  - Multi-Specialty Group Practice / Community Health Mission
  - US Family Health Plan (DoD Sponsored)
  - 1000+ infrastructure & network devices
  - Business Partners include major Hospital, Imaging Center, Transcription Service, Laboratory, EDI VAN

# PMC Required to Undergo DITSCAP Certification

- TriWest Healthcare Alliance, a records company that is part of DOD's TriCare system, announced that its Phoenix offices had been broken into Dec. 14 and that computers and files were stolen.
- The Phoenix contractor for the Defense Department's medical system is offering a \$100,000 reward for information that helps lead to the arrest and conviction of perpetrators who stole computers containing thousands of medical records.
- Contained on those systems are the confidential and personal files of more than 500,000 members, who are active-duty military, retirees or their families. The information stolen includes names, addresses, Social Security numbers and other personal information, such as diagnoses.

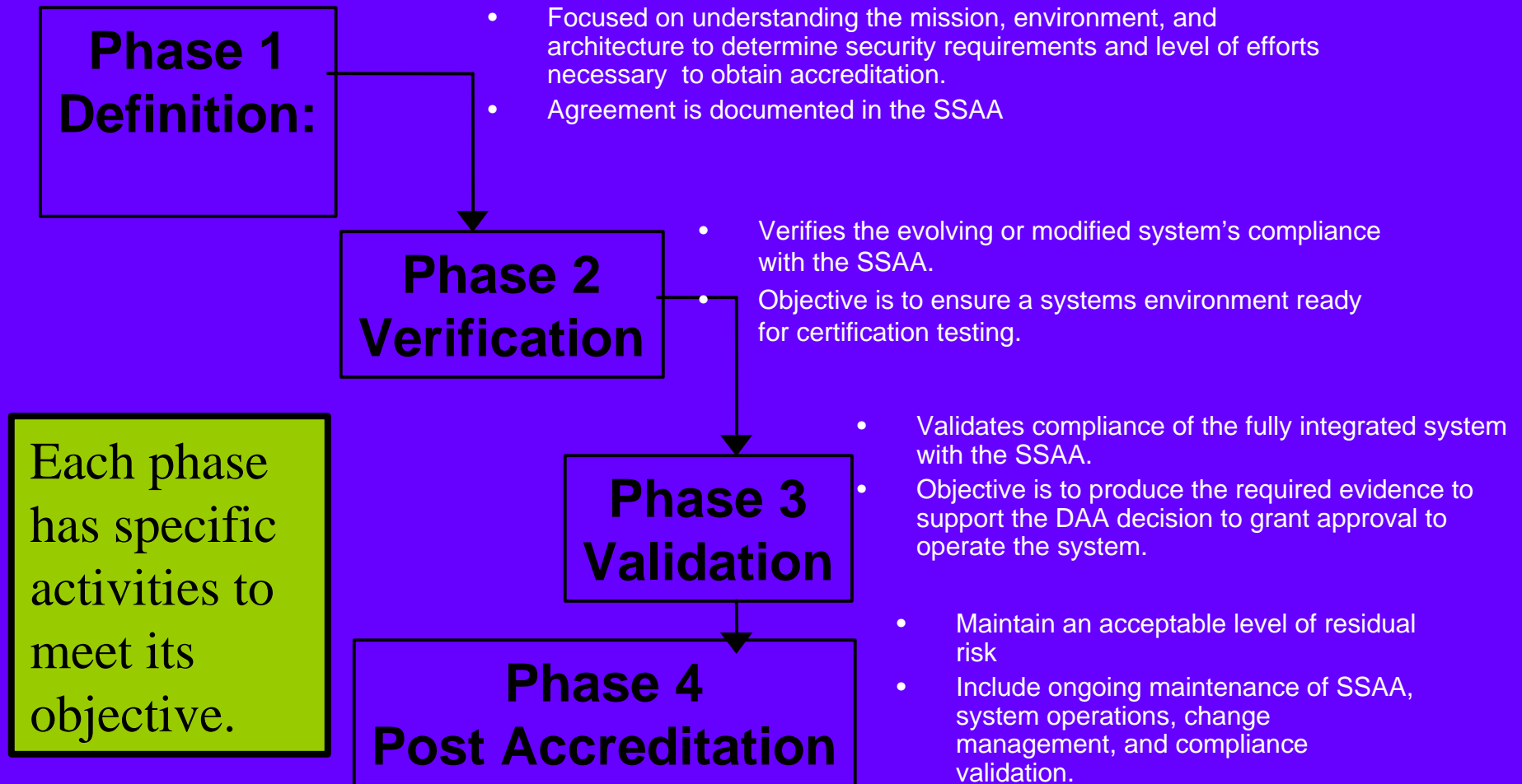
*Federal Computer Weekly Jan. 3, 2003*

***As a result of the TriWest data theft all 7 US Family Health Plan (USFHP) healthcare companies around the United States are required to attain DITSCAP certification prior to being afforded a final Authority To Operate (ATO)***

# DITSCAP: HIPAA Security on Steroids

- Defense Information Technology Security Certification & Accreditation Process
  - DoD standard for protecting and securing information systems comprising Defense Information Infrastructure (DII) / based upon National Security Agency guides.
  - Process for certifying that target systems are safe to operate.
  - Ensures target system maintains accredited security posture for entire lifecycle.
  - Information and Network Boundaries Clearly Identified
  - ***Addresses Physical, Administrative, and Technical Information/Infrastructure just like HIPAA Security Rules***

# DITSCAP: Multiple Phases



April 6-8, 2005

10<sup>th</sup> National HIPAA Summit

# Advantages of DITSCAP

- Ensures vulnerabilities are addressed to the extent that **ALL** residual risks are reduced.
- Security activities must be tailored based on **mission and risk strategy**.
- Facilitates identification of **achievable security solutions**
- Forces honest appraisal of internal capabilities and **ability to sustain security posture**

# Surviving DITSCAP or HIPAA Remediation

- 12 weeks from Phase 2 to Phase 4
- Phase 2: DoD & iTM teams performed full assessment of facilities and infrastructure in an 10X24 time-frame
  - Security Assessment Raw Data
  - 6,000+ pages of data left with PMC: 58,000+ vulnerabilities
  - Dod team delivered report 3 weeks later with matrix of 940 discrete vulnerabilities
  - No tools to manage data—had to build management tools
  - Multiple vulnerability tracks had to synchronize planning
- Phase 3: 8 weeks after assessment DoD team arrives and conducts verification assessment
  - Expectation: **0 vulnerabilities unmitigated** (High/Medium/Low)
  - Expectation: All vulnerabilities documented with “evidence” of remediation
  - Results: **10 Low Vulnerabilities all mitigated**
- How did PMC achieve: dedication, determination, augmented staff, technology upgrades & migration from NT to Win2000, desktop standardization? Lots & Lots of effort (\$), Lots & Lots of patience and understanding from all staff.

# Real Benefits of DITSCAP to PMC

- Ensured **ALL** Facilities/Clinics were assessed and vulnerability **remediation steps completed**.
- Assessed all databases and application systems and hardware and subsequently **certified all vulnerabilities were remediated**.
- **“HIPAA Addressable” requirements became DITSCAP “Required” best practice solutions.**
- **Third and Fourth Party assessment of overall Infosec strategies** and evaluation of PHI exchange mechanisms that resulted in vast improvements in secure connectivity with business partners.
- **Documentation of policies, procedures, security zones, network boundaries, etc.**

# Compelling Considerations

[Healthcare] IT organizations **[must]** question whether [their] solutions vendors have sufficiently robust security practices and if vendors can meet the internal security requirements .... The risk of security breaks or intellectual property protection is inherently raised when working in international / global/ outsourced business.

Privacy concerns must be completely addressed. Although these issues rarely pose major impediments to outsourcing, the requirements must be documented and the methods and integration with vendors defined **[with independent third party verification and validation on a frequent basis]**

*February 2004 - Source: Metagroup*

# Does bin Laden have US Army medical files?

## *Asheville woman blows whistle; company denies story*

Could Osama bin Laden and other terrorists have access to the medical records of thousands of retired and active duty American military personnel? That's one possibility according to a story of overseas outsourcing, broken promises, corporate intimidation and massive technological failure told by a former employee of the medical transcription company.

The employee said the company had contracted with the Veterans Administration to transcribe voice dictation from doctors at Veterans Administration Medical Centers around the world...some of this transcription work has been done by offshore workers in India and Pakistan.

*Asheville Tribune, 2004*

# Current Security Landscape

- It's more than adding a firewall, IDS, or log analyzers
- Spyware is the new SPAM—and it can be much more damaging
- Phishing—no one is safe from it
- **Databases are the real targets now!**
- Viruses—Time from vulnerability discovery to exploit is now measured in days or hours
- External Hackers—Perimeter security has lessened, but not eliminated these threats
- **Internal Hackers—Many organizations are not prepared**
- ActiveX Control vulnerabilities
- Lack of start-up boot controls on floppies, USB
- Lack of HR Termination/IS Security link

# Current Security Landmines

- Tools/Processes
  - Microsoft has progressed with security management, but will always be targeted because of market share
  - Patch management is difficult at best—too many patches cause as many problems as they fix
  - Vulnerability scanning tools are cumbersome, require constant updating and management
    - ISS Toolkit Robust but Difficult to Use and comprised of many disparate solutions
    - Qualys Appliance Easy to use but limited to physical Devices
    - One toolkit not likely to provide total coverage at this time
    - Integration with current Problem Ticketing an issue
  - It is more than Windows Patches!!!
- Security Assessment Vendors
  - All say they are qualified to perform vulnerability assessments, but it's more than a network assessment!
  - Healthcare Facility security assessment is new

## Mobile Devices Are Enterprise Security Risk

The threat that mobile devices pose to enterprises is significant, yet a significant majority of organizations haven't deployed systems to manage those devices, according to a Forrester study

*USA - August 20, 2004 - Source: Mobile Pipeline News*

# It's Only a Matter of Time

- Risk Management is key
  - Must look at the impact to the business
  - External review/certification doesn't eliminate risk—but may help mitigate it
- Constantly review policy and procedures
- Technology is simply a tool—process and culture change are the real drivers
- New Technology=New Unknown Threats

# What About Portable Patient Health Records

## Consider the problems with this approach!

- Establishing new infrastructure models will take time; especially in the healthcare IT world. In order to get started, a patient can begin creating their own Personal Health Record (PHR). The ideal PHR software application will enable patients to create—among other things—a personalized emergency file.
- A USB Flash drive used in conjunction with the PHR will be able to detect when it is plugged into the “home” computer or into an unknown computer. If it is plugged into an unknown computer, the software on the USB drive assumes that it is being inserted into a computer of an Emergency Room (ER).
- The application will immediately pull up and present to the viewer the emergency medical information. The patient creates the emergency file with the understanding that it will not be protected or secure. The file is not protected so as to allow ER personnel to access the data if a patient is unconscious.

*This approach needs serious SECURITY tooling*

# Terra Incognita

- Healthcare EMR/HIS/CDR vendors security assessment
- Portable Health Record—technically possible, politically difficult
- PDA and USB devices
- VOIP Integration and Security Issues
- Wireless Security Improvements
- Viruses, SPAM, and other threats will continue unabated
- Tools will continue to improve, but will struggle to keep up with requirements
- Security requirements will continue to increase—HIPAA will mirror DITSCAP
- **Mandatory CERTIFICATION ???**

# Organizational Implications

- Provider Organizations: workflow will be impacted in many areas where there are shared devices until better technology is adopted for “sign-on”
- Payer Organizations: follow the money....ID Theft
- Single-sign-on brings its own Security and Operational Issues
- More money **HAS TO BE** allocated for Security across the organization: Physical / Administrative/ Technology
- More Security Professionals With Real Authority
- Role-based system access Improvements
- Liability and Risk: Would a third party consider your efforts reasonable?
- Decisions made today will affect tomorrow!
- **Security is the journey, not the destination**

# CIO Magazine Security Survey 2005

	<u><i>Best Practice</i></u>	<u><i>Overall Survey</i></u>
<i>Budget for Security</i>	14%	11%.
<i>Security Staffing</i>	20/1000 employees	14/1000
<i>Organizational Structure</i>	CPO 27% CISO 25%	CPO 20% CISO 16%

CPO Chief Privacy Officer  
CISO Chief Information Security Officer

# Why Too Little, Too Late?

- Security rules are already obsolete
- Read the newspapers: Unthought-of Security Breaches occur daily in every industry
- HIPAA doesn't require CERTIFICATION
- Civil and Criminal penalties Need Boosting
- Too many items left as ADDRESSABLE
- Healthcare Application Security models need updating
- Healthcare solution vendors must address security concerns equal to interoperability issues

# Call on Government To Study Health IT Security



The National Committee on Vital and Health Statistics called for the government to assess potential security risks from the use of electronic prescribing and health care information technology. **Experts say ensuring the security of digital health information is necessary to persuade the public to support health IT.**

Although HIPAA includes some data-security provisions, the **regulations do not set a minimum security standard** that health care organizations should provide...**The rules only represent steps that providers can follow to show they are making a "good-faith effort to protect data"**

The NCVHS also called for HHS and the Department of Justice to discuss ... standardization of electronic signatures...and requiring health care organizations to use an **"unnecessarily high level of security" with e-prescribing would make using the technology too expensive and thereby negate its cost benefits** (Bazzoli, *Healthcare IT News*, 3/14).

# Questions?

Please feel free to ask any questions now or catch us after the presentation.

Thank you for coming!