

Compliant with HITECH's Data Breach Notification Mandate?

Addressing HIPAA Audit Requirements



Ali Pabrai, MSEE, CISSP (ISSMP, ISSAP)
Author, Precision Security (Forthcoming)
Member, FBI InfraGard

Agenda

- Examine key requirements for the HITECH's data breach notification
- Identify who needs to be informed – key processes & capabilities required
- Understand concept of “unsecured PHI” and its impact on policies and processes for data breach management
- Understand how to prepare for an audit by organizations such as the OCR
- Identify critical steps to address data breach notification requirements of the HITECH Act

Data Breach Reach New Heights

- Cost of data breach rose to \$202 for each compromised record
- Average cost of healthcare breach was \$282 for each record
- Average expense to an organization was \$6.6 million
- Vast majority caused by negligence
- Portable devices, laptops are responsible for growing # of breaches

Source: The Wall Street Journal, February 2, 2009

How prepared is your organization?

Information - The New Currency of Business

Global State of Information Security – PWC Report 2008

- Most organizations do not know where their most important data is located
- From protecting privacy to improving safeguards – organizations are struggling
- Greatest risk to sensitive corporate information is that a user with either legitimate or unauthorized access will compromise data – intentionally or accidentally
- Data breaches are really damaging
 - Financial losses, Theft of IP, Compromise of brand, Fraud
- Nearly 50% of respondents can't identify vulnerabilities that led to security incidents!
- Employees & former employees remain biggest threat!

What is the risk to information assets?

How confident are you about your organization's information security posture?



Key Definitions

ARRA & HITECH Act

Breach

The term “breach” means the unauthorized acquisition, access, use, or disclosure of Protected Health Information (PHI) which compromises the security or privacy of the PHI such that it poses a significant risk of financial, reputational, or other harm to the individual

Unsecured PHI

PHI that is not secured through the use of a technology or methodology specified by the Secretary of HHS; PHI must be rendered *unusable, unreadable, or indecipherable* to unauthorized individuals

Privacy & Security Breaches

HITECH Act Requirements

- Covered entities must notify individuals whose unsecured PHI has been or is reasonably believed to have been *accessed, acquired* or *disclosed* as a result of a privacy or security breach
- If the breach is discovered by a business associate then the business associate is required to notify the covered entity of the breach
 - Including providing information about the identification of each individual who has been or is reasonably believed to have been affected by the breach
- Breach notices must be sent without unreasonable delay and in no case later than 60 calendar days after discovery
- A breach is “discovered” on the first day on which such breach is known to the covered entity or the business associate
- If breach involves more than 500 residents of a state, then prominent media & Secretary of HHS must be sent notice



Business Associates

New Mandates

Business associates:

- Are now subject to the administrative, physical and technical safeguard security requirements of the HIPAA Security Rule
- Must develop policies, procedures and documentation of security activities
- Are prohibited from making any use or disclosure of PHI that is not in compliance with each of the required terms of a HIPAA BAA
- That violate the HIPAA Security Rule or the terms of the BAA are now subject to the same civil and criminal penalties as covered entities

Health Information Exchanges (HIE):

- Are business associates and must enter into a BAA with the covered entity



New Penalties

HITECH Act

The Act defines tiers of penalties:

- **Tier A** – *if the offender did not know*
 - \$100 for each violation, total for all violations of an identical requirement during a calendar year cannot exceed \$25,000
- **Tier B** – *violation due to reasonable cause, not willful neglect*
 - \$1,000 for each violation, total for all violations of an identical requirement during a calendar year cannot exceed \$100,000
- **Tier C** – *violation due to willful neglect, but was corrected*
 - \$10,000 for each violation, total for all violations of an identical requirement during a calendar year cannot exceed \$250,000
- **Tier D** – *violation due to willful neglect, but was NOT corrected*
 - \$50,000 for each violation, total for all violations of an identical requirement during a calendar year cannot exceed \$1,500,000



Notification Methods

- Written notice to the individual by mail or email
- In case of 10 or more individuals for which there is insufficient information, conspicuous posting on the *home page of the Web site* or notice in *major print or broadcast media*
- If *imminent misuse* suspected then by phone in addition to methods above
- Prominent media outlets within the State or jurisdiction informed if breach impacts more than 500
- Secretary of HHS for breaches involving more than 500; annually for all other breaches
 - Posting by HHS on their web-site of breaches involving more than 500 individuals



Methods for Securing PHI

- The guidance document from HHS identifies two methods for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals
 1. Encryption
 2. Destruction
- The successful use of encryption depends upon two main features:
 1. The strength of the encryption algorithm
 2. Security of the decryption key or process
- Destruction of PHI
 - Paper - Shredded or destroyed such that PHI cannot be read or reconstructed
 - Electronic – Cleared, purged, or destroyed such that PHI cannot be retrieved



Audit Guidance for HIPAA

Preparing for Audits by OCR & Others

- Entity-wide Security Plan
- Risk Analysis (most recent)
- Risk Management Plan (addressing risks identified in the Risk Analysis)
- Security violation monitoring reports
- Vulnerability scanning plans
 - Results from most recent vulnerability scan
- Network penetration testing policy and procedure
 - Results from most recent network penetration test
- List of all user accounts with access to systems which store, transmit, or access EPHI (for active and terminated employees)
- Encryption or equivalent measures implemented on systems that store, transmit, or access EPHI

Visit www.pabrai.com for details.



Audit Guidance for HIPAA Policies – Approved and Implemented?

- Prevention, detection, containment, and correction of security violations
- Employee background checks and confidentiality agreements
- Establishing user access for new and existing employees
- List of authentication methods used to identify users authorized to access EPHI
- List of individuals and contractors with access to EPHI to include copies pertinent business associate agreements
- List of software used to manage and control access to the Internet
- Detecting, reporting, and responding to security incidents
- Physical security
- Encryption and decryption of EPHI
- Mechanisms to ensure integrity of data during transmission - including portable media transmission



Audit Guidance for HIPAA Procedures Updated and Functional?

- Monitoring systems use - authorized and unauthorized
- Use of wireless networks
- Granting, approving, and monitoring systems access (for example, by level, role, and job function)
- Sanctions for workforce members in violation of policies and procedures governing EPHI access or use
- Termination of systems access
- Session termination policies and procedures for inactive computer systems
- Policies and procedures for emergency access to electronic information systems
- Password management policies and procedures
- Disposal of media and devices containing EPHI
- Secure workstation use



Ready to be Interviewed for an Audit?

Partial list includes:

- Executives
- HIPAA Officer
- Security Officer
- Systems Management
- Network Engineers
- Disaster Recovery Coordinator
- Incident Response Team
- Other IT resources
- Physical (Facility) Security
- Human Resources (HR)
- Director of Training



State Regulations

Taking Breaches Further

California

- **SB 1386** requires notification of security breaches involving “unencrypted” sensitive data
- **AB 1950** requires that organizations take “reasonable precautions” to protect CA residents’ personal data
- **AB 1298** expands data breach notification law to include unencrypted medical histories, health insurance information, medical treatments & diagnoses
- **SB 541** requires breaches must be disclosed to the affected patients
- **AB 211** includes fines starting from \$2,500 to \$25,000 per violation for organizations that negligently disclose patient records

Massachusetts

- **201 CMR 17.00** establishes minimal standards for safeguarding personal information contained in both paper and electronic records



Case Study: What the FTC Expects! Notice of Breach of Health Information

Under the law 16 CFR Part 318, organizations must:

- Notify everyone whose information was breached
- In many cases, notify the media; and
- Notify the FTC

Timelines

- Breaches \geq 500, Information sent to FTC within 10 business days of discovering breach
- Breaches $<$ 500, Send information to FTC by the 60th day following the breach

Information FTC expects to receive

- Type of breach
- Date of breach, date breach was discovered
- # of individuals impacted by the breach

Case Study: What the FTC Expects!

Type of Information Involved in Breach

Personal Information

- Name, Address, Date of Birth, SS#, Driver's license or id card #
- Financial information (cc, bank account # etc.)
- Health insurance information (insurance carrier, insurance card # etc.)

Health Information

- Basic information (age, sex, height etc.)
- Disease or medical conditions, Medications
- Treatments or procedures, Immunizations
- Allergies, Test results, Hereditary conditions
- Information about children
- Mental health information
- Information about diet, exercise, weight etc.
- Living wills, medical power of attorney
- Organ donor authorization



HITECH to HIPAA

Be Audit Ready, Always!

The Seven Steps to Enterprise Security™



Critical Action

Conduct Privacy & Security Gap Analysis



ecfirst's HITECH Data Breach Solutions

ecfirst Data Breach Preparation helps an organization prepare for the HITECH and state breach notification regulations by:

Developing an EPHI Breach Identification & Notification Policy

Developing an EPHI Breach Technical/Operational Procedure

Developing Data Breach Notification Templates

Identifying Current Capabilities to Detect an EPHI Data Breach

Recommending Needed Improvements

Conducting a 1 hour Training Webinar



About ecfirst

Delivering Value with Integrity

Industry leader delivering world-class services in the areas of compliance and information security for a decade

Recognized as an Inc. 500 Business in 2004



Certified Targeted Small Business

Unique, business-driven, compliance and security solutions; based on proprietary BizShield™ methodology

er 1,400 Clients served including Microsoft, McKesson, HP, Symantec, PNC Bank, hundreds of hospitals, government agencies and more...



Compliance & Security

Getting Started

- Conduct – complete - the following requirements
 - HIPAA Privacy Gap Analysis
 - HIPAA Security Risk Analysis (*Specified in CMS HIPAA Audit Guidance*)
 - Technical Vulnerability Assessment (*Specified in CMS HIPAA Audit Guidance*)
 - HITECH Data Breach Risk Assessment, Policy and Procedures
- Now available in the ecfirst e-store for you to download:
 - HITECH, HIPAA, ISO quick reference cards
 - Privacy & Security Policy Templates
 - ISO 27002 to HIPAA Matrix (Mapping)
- Schedule a call to discuss next steps
 - Bring ecfirst to your site for training and consulting services
 - Contact Lorna Waggoner at 1.515.453.8247 x17 or at Lorna.Waggoner@ecfirst.com

Precision Security by Pabrai

Pre-order your copy. Expected Dec 21, 2009

