How HIPAA Fits into the Broader Scheme of Privacy & Security Regulations

Ali Pabrai, **CISSP (ISSAP, ISSMP)**
Member, FBI InfraGard

Technology Challenges

- Complex Computing Environment
  - ❑ Too many servers, too many applications
  - ❑ Too many credentials across multiple systems to manage
  - ❑ Too many end systems to support and maintain
  - ❑ Mobility of devices is rapidly increasing
  - ❑ Storage demands are rising fast
  - ❑ Highly specialized technical skills required
  - ❑ Serious lack of redundancy in infrastructure
  - ❑ Struggle with resources to monitor and audit

Security Challenges

- Struggling with fast, secure access to patient information
  - Patient information is spread across several applications
- Generic accounts still in active use
- Struggling with password management
- Need to uniquely identify “who accessed what, when, how”
- Audit controls are not consolidated and typically not automated, nor complete
- **Important References**
  - ISO 27000 (ISO 27001, ISO 27002) – international security standard
  - NIST Standards (SP 800-66 Rev 1)

Compliance Challenges

- Key Regulations
  - ❑ HIPAA Privacy
  - ❑ HIPAA Security
  - ❑ HITECH Act
  - ❑ FACTA (Red Flags Rule)
  - ❑ State Regulations
  - ❑ PCI DSS

Data Breach Reach New Heights

PII is at Risk

- 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 in securing PII?

PII is a Board Level Priority

HIPAA and HITECH Mandate

Key Definitions

ARRA & HITECH Act

Breach

The term ‘‘breach’’ means the *<u>unauthorized acquisition, access, use, or disclosure</u>* of Protected Health Information (PHI) which compromises the security or privacy of the PHI such that it poses a *<u>significant risk of financial, reputational, or other harm</u>* 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 *<u>unauthorized individuals</u>*

Meaningful Use & HIPAA | HITECH

- Compliance with HIPAA's Privacy & Security Rules remain part of the meaningful use definition as a policy priority, with corresponding goals and objectives for 2011
- CMS will withhold meaningful use payment for any entity until any confirmed HIPAA privacy or security violation has been resolved
- Further, state Medicaid administrators will withhold meaningful use payment for any entity until any confirmed state privacy or security violation has been resolved

EHR initiatives are coupled with increased privacy and security compliance with mandates

FISMA

- The Federal Information Security Management Act (FISMA) requires each U.S. federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems
- These systems include those that support the operations and assets of the agency
- U.S. federal agencies must be compliant with FISMA requirements
- The FISMA legislation is about protecting information and information systems from unauthorized:
  - ❑ Access
  - ❑ Use
  - ❑ Disclosure
  - ❑ Disruption
  - ❑ Modification
  - ❑ Destruction
- FISMA is all about information security

State Regulations

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

Over 40 States Now Have Security Regulations!

Preventing <u>unauthorized access</u>, <u>encryption</u> & <u>audit trails</u> are key!

Massachusetts 201 CMR 17.00

Comprehensive Written Information Security Program Required

- Establishes minimal standards for safeguarding personal information contained in both paper and electronic records
- Requires each covered business to “develop, implement, maintain and monitor a comprehensive written information security program” that applies to records that contain Massachusetts’ residents’ personal information
- Security program must include “administrative, technical and physical safeguards” to protect such records
- Regulations also require businesses that store or transmit personal information about Massachusetts’ residents to (201 CMR 17.04):
  - Restrict access by use of passwords
  - Deploy updated malware protection
  - Encrypt information transmitted across public or wireless networks
  - Monitor all systems to detect unauthorized access
  - Encrypt information stored on laptops
  - Incorporate firewalls

Nevada

Ensure Transmission Security

- Nevada law provides that “a business in this State shall not transfer any personal information of a customer through an electronic transmission (except fax) to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission
- Personal information is defined as a person’s name together with SSN, a driver’s license #, financial account # plus PIN, or other code to gain access to an account

FACTA

Fair and Accurate Credit Transactions Act

- FACTA is a U.S. federal law
  - Signed by President Bush on December 4, 2003
- FACTA is an amendment to the Fair Credit Reporting Act (FCRA)
- The Act includes provisions to reduce identity theft
- FACTA instituted a procedure to help users of consumer reports address identity theft by creating the concept of “red flags” when identity theft is suspected

Health care providers – whether they are for profit, non-profit, or government entities – may be impacted by the Red Flag regulations, the *Red Flag and Address Discrepancy Rules*

PCI DSS & Healthcare

A Global Data Security Standard

1. **Build and Maintain a Secure Network**
    1. Firewall configuration
    2. Vendor defaults
2. **Protect Cardholder Data**
    3. Protect stored cardholder data
    4. Encrypt transmission
3. **Maintain a Vulnerability Management Program**
    5. Update anti-virus software
    6. Maintain secure systems and applications
4. **Implement Strong Access Control Measures**
    7. Restrict access – need to know
    8. Assign unique ID's
    9. Restrict physical access
5. **Regularly Monitor and Test Networks**
    10. Track and monitor all access
    11. Regularly test security processes
6. **Maintain an Information Security Policy**
    12. Maintain policies

Healthcare organizations are likely impacted and must comply

NIST 800-37 Rev 1

- Developed by NIST to comply with FISMA responsibility
- *Guide for Security Authorization of Federal Information Systems (NIST SP 800-37 Rev 1)*
  - *A Security Life Cycle Approach*
- A common *security authorization process* for federal information systems
- A well-defined and comprehensive security authorization process that helps ensure appropriate entities are assigned *responsibility and are accountable for managing information system-related security risks*

FIPS 199

- Title III of the E-Government Act of 2002 entitled the FISMA-tasked NIST with responsibilities for standards and guidelines including:
  - Standards to categorize all information and systems (FIPS 199)
  - Guidelines recommending types of information and systems
  - Minimum information security requirements (controls for each category (established in FIPS 200)
- **FIPS 199 is the standard to categorize information and information systems**

FIPS 200

- FIPS 200 establishes the minimum security requirements for federal information and information systems
- This standard establishes the minimal requirements in seventeen security-related areas
- Federal agencies are required to meet the minimal requirements through the use of security controls in accordance with NIST SP 800-53
- **FIPS 199 and FIPS 200 are the first of two mandatory standards required by the FISMA legislation**

NIST SP 800-34

Contingency Planning

1. Develop a Contingency Planning Policy
2. Conduct Business Impact Analysis (BIA)
3. Identify preventative measures
4. Develop recovery strategy
5. Develop the Contingency Plan
6. Conduct testing and training
7. Review and maintenance

Contingency Plan – A HIPAA Security Rule Standard
Organizations are struggling to address!

ISO 27000: An International Security Standard

- A comprehensive set of controls comprising best practices in information security
- Comprised of:
  - ❑ A code of practice
  - ❑ A specification for an information security management system
- Intended to serve as a single reference point for identifying a range of controls needed for most situations where information systems are used in industry and commerce

Healthcare organizations, especially business associates, are looking at the ISO 27000 as a security framework to address HIPAA Security, PCI DSS, State mandates

Beyond PHI. PII.

Personally Identifiable Information

Until now, it has been about

- Protected Health Information (PHI) – *HIPAA Privacy*
- Electronic Protected Health Information (EPHI) – *HIPAA Security*
- Unsecured PHI – *HITECH Act*
- Cardholder information – *PCI DSS*
- Personal data or information – *State Regulations*

2010 and beyond – it is about PII

- What PII does your organization come into contact with?
- Where is PII in your organization?
- How is the PII secured in your organization?

Case Study: What HHS Expects!

Notice of Breach of Unsecured PHI

Organizations must:

- Identify if breach affects 500 or more OR Less than 500
- Initial Report, Addendum to Previous Report
- Provide covered entity contact information
- Identify if breach occurred at or by a Business Associate

Breach

- Date of breach, Date of Discovery, Approx # of impacted individuals

Type of Breach

- Theft, Loss, Improper disposal, Unauthorized access, Hacking/IT incident
- Other, Unknown

Type of PHI Involved in Breach:

- Demographic information, Financial information, Clinical Information, Other

Case Study: What the HHS Expects!

Notice of Breach of Unsecured PHI

Brief Description of Breach

- Location, How it occurred?
- Additional information: type of breach, type of media, type of PHI

Safeguards in Place <u>Prior</u> to Breach

- Firewalls, Packet filtering (router based)
- Secure Browser Sessions, Logical Access Control
- Strong Authentication, Encrypted Wireless, Physical Security
- Anti-virus Software, Intrusion Detection, Biometrics

Action in Response to Breach

- Security and/or Privacy Safeguards. Mitigation
- Sanctions, Policies & Procedures, Other

Attestation

Breach Policy & Procedures

Getting Started…

- Develop a formal policy on Discovery, Reporting and Notification of Information Breaches
- Create a specific procedure for information breach management
  - ❑ Who will manage the phases of the process once a breach has been identified?
  - ❑ Who are the individuals involved in managing the process?
  - ❑ Identify all systems impacted or compromised for further investigation
  - ❑ Inform law enforcement as appropriate
  - ❑ Establish what federal and state regulations are applicable to the incident
  - ❑ Organize all associated documentation
- Develop specific procedure for information breach notification
  - ❑ Determine the required notification for the patient or impacted individual
  - ❑ Determine if media needs to be informed and if so establish the required notification for media
  - ❑ Determine if HHS needs to be informed and establish the process

PII – A Checklist of What You Must Address

1. Has the organization clearly identified all PII residing in the enterprise?
2. Has the organization categorized PII?
3. Are you applying appropriate safeguards based on confidentiality impact level?
4. Is the collection and retention of PII limited to what is strictly necessary?
5. Have you developed an incident response plan to handle breach of PII?
6. Has the organization established a “forum” to enable close coordination between privacy officers, CIO, security officers and legal?

This checklist must be completed on a regular schedule

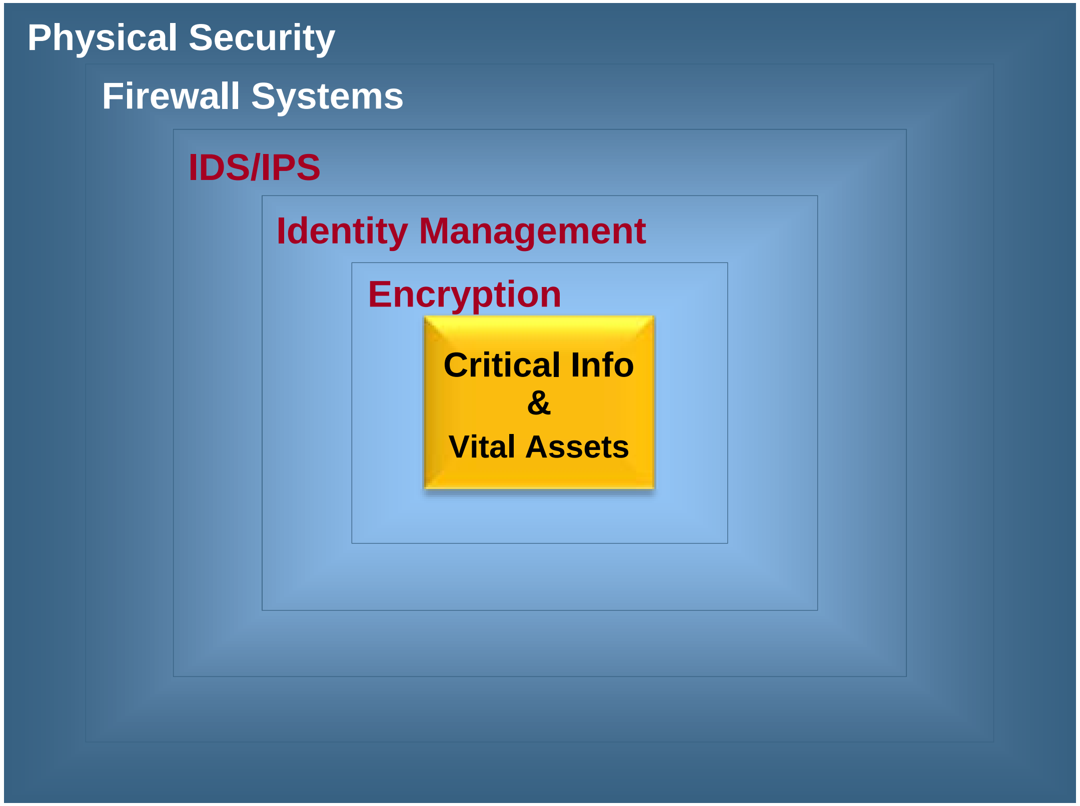
Incident Response for Breaches of PII

Four Key Phases

1. **Preparation**
    1. Build PII breach response as part of incident response
    2. Develop appropriate policies & procedures
    3. Employees must understand what constitutes a PII breach
    4. Develop a comprehensive breach notification plan
2. **Detection and Analysis**
    1. Implement detection & analysis technologies & techniques
    2. Make adjustments as needed
3. **Containment, Eradication & Recovery**
    1. Perform additional media sanitization steps
    2. Ensure proper forensics techniques are practiced
4. **Post-Incident Activity**
    1. Learn and update PII breach response plan

Information Security Program Strategy

Core to the Edge and the Cloud



Physical Security

Firewall Systems

IDS/IPS

Identity Management

Encryption

Critical Info
&
Vital Assets

Security Strategy Must be Risk-based, Pro-active, Integrated!

Thank You!

CSCS™

CERTIFIED SECURITY COMPLIANCE SPECIALIST

- CHP + CSCS Certification – ILT & On-line
  - 4 Days, 2 Valued Credentials
- Exclusive HIPAA/HITECH Solutions from ecfirst include:
  - Managed Compliance Services Program (MCSP) for HIPAA
  - 1-hour Webcast to 4-Day Training Programs
  - HIPAA & HITECH Policy Templates
  - ISO 27002 to HIPAA Matrix (Mapping)
- Do keep in touch
  - Bring ecfirst to your site for compliance and security challenges
  - P: 1.949.260.2030, or E: Pabrai@ecfirst.com

New! On-Demand Consulting Service**.**

Min. 40 hour block. Fixed Price. 2-page Contract.

ecfirst