Checklist for HIPAA/HITECH Compliance

Best Practices for Healthcare Information Security

Ali Pabrai, MSEE, CISSP (ISSMP, ISSAP)

For Daily Compliance & Security Tips, Follow ecfirst @

Agenda

- Review the *key areas* that must be addressed to ensure HIPAA & HITECH compliance on a *continual* basis
- Explore the critical policies & associated controls for *breach management*
- Discuss the use of a system security plan to establish the foundation for a *comprehensive information security program*

Rising Risk to Business

Risk to Information is a Risk to Business

A Single Incident/Breach

Significant Risk!

- Hackers broke into the computer system of the United Nations and hid there unnoticed for almost two years, and quietly combed through reams of secret data

  McAfee, August 2012

- Hackers gained unauthorized access to the internal Zappos network and its 24 million customer accounts
  - "We spent over 12 years building our reputation, brand and trust with our customers. It is painful to see us take so many steps back due to a single incident." Mr. Tony Hsieh, Zappos, CEO

    The Wall Street Journal, January 17, 2012

Data Breach:

- $4.9 Billion Class-Action Lawsuit, TriCare/SAIC
- 4.9 million records lost, unencrypted backup tapes stolen

ecfirst

Your Org Next?

UCLA Health System

- In Nov 2011 reported that a hard drive containing more than 16,000 patients' information had been stolen from the home of a UCLA physician on Sept. 6, 2011
  - Lawsuit filed claims the incident was a violation of the California Confidentiality of Medical Information Act; calling for $1,000 in damages for each patient impacted by the incident
- OCR investigated in June 2009 after receiving separate complaints from two celebrity patients of unauthorized access to their records
  - Discovered that from 2005 to 2009 unauthorized employees repeatedly looked at the EPHI of numerous UCLA HS patients
  - The investigation further found that the UCLA HS failed to implement sufficient security measures or document appropriate training or sanctions
  - UCLA HS settled potential HIPAA violations with OCR for $865,500 and agreed to a multi-step corrective plan over the next three years
- UCLA was fined $95,000 in 2009 by CDPH for breaches involving pop singer Michael Jackson's death

Hacker releases 100,000 Facebook log-in credentials!
IDG News, Jan 24, 2012

ecfirst

Breaches

Not If, But When!

- Response will be costly; especially notification!
- Is your strategy for incident response management and breach aligned? Tested?
- Employees trained on policies? Incident response team prepared? Controls deployed?
- Addressed federal and state breach mandates?

As of January 1, 2012, California requires significantly more information to be included in data breach notification letters to CA residents

963,434 cyber attacks in October 2011! SC Magazine, Nov 2011

ecfirst

OIG Findings: Security Weaknesses

Areas of Concern Identified in Report

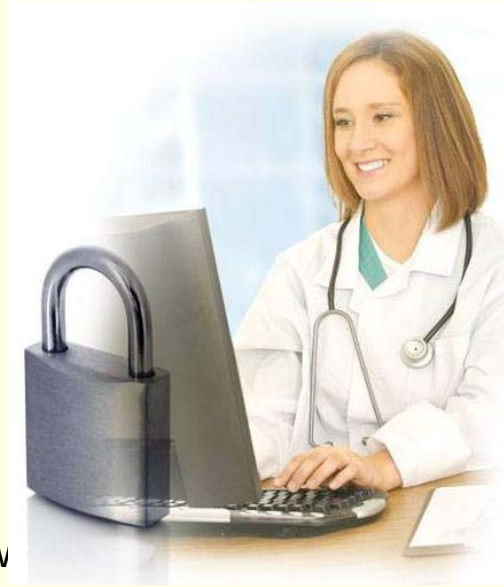
- Examples of weaknesses identified by the OIG @ hospitals included:
  - Unprotected wireless networks
  - Lack of vendor support for operating systems
  - Inadequate system patching
  - Outdated or missing antivirus software
  - Lack of encryption data on portable devices and media
  - Lack of system event logging or review
  - Shared user accounts
  - Excessive user access and administrative rights

External threats rising daily… highly targeted & persistent
Can your Security Strategy defend these threats?

ecfirst

Health IT Challenges

- Healthcare – Complex Computing Environment
  - Cloud computing
  - Virtualization
    - Servers
    - Desktop
  - Mobile devices
  - TBs of data across several storage media
- Security – PII is at Significant Risk!
  - Struggling with fast, secure access to patient information
  - 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



Risk to PII is a Risk to the Organization!

ecfirst

Compliance Mandates

- Key Regulations & Standards
  - HIPAA Privacy
  - HIPAA Security
  - HITECH Meaningful Use
  - HITECH Breach Notification
  - State Regulations
  - PCI DSS

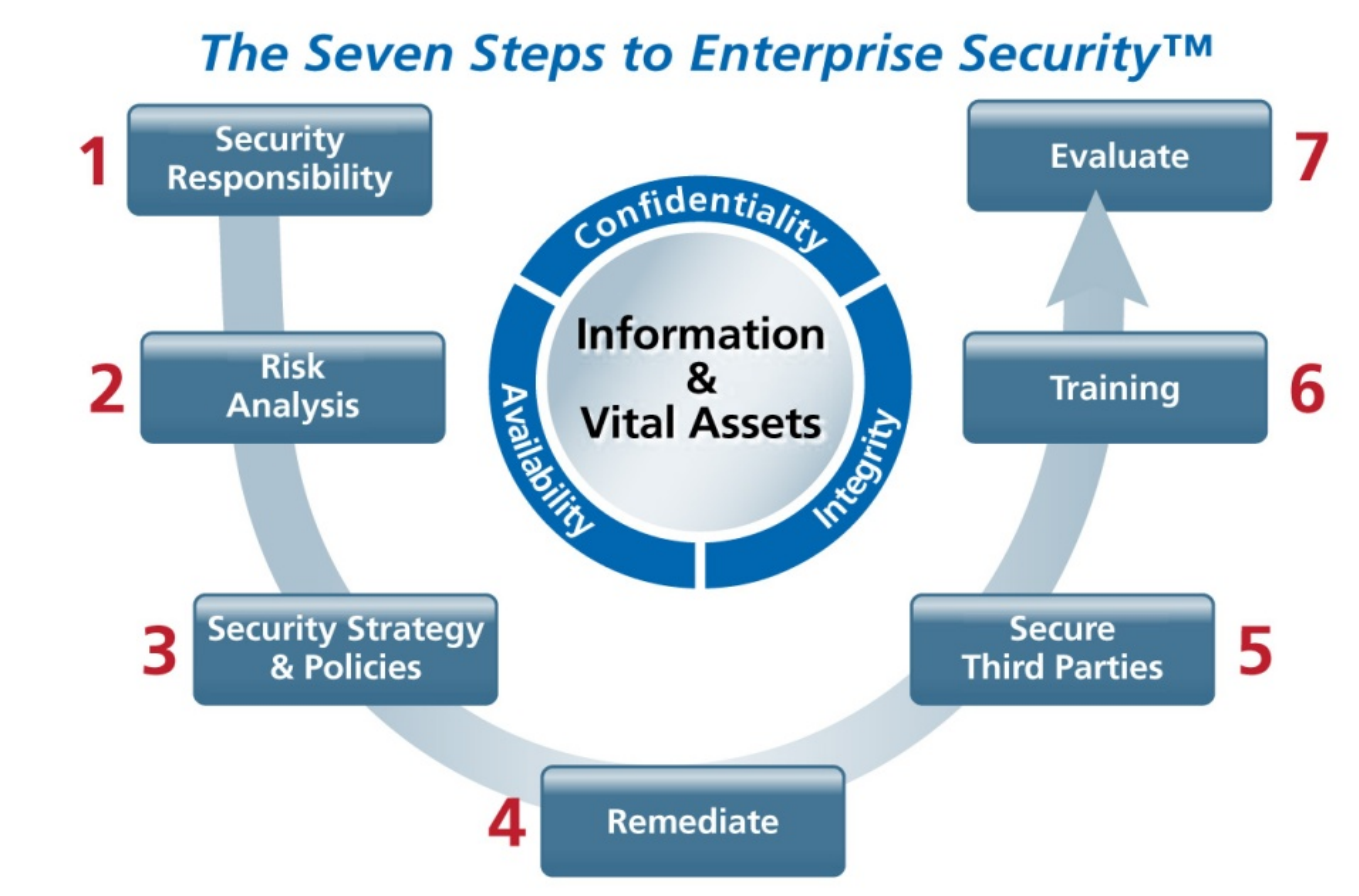
Your security plan must identify regulations that impact your organization!

ecfirst

Best Practices

A 7-Step Checklist!

Establish a Security Program!



bizSHIELD™

ecfirst

Prepared for an Audit?

Documentation Recently Updated?

- Entity-wide Security Plan
- Risk Analysis
- Risk Management Plan
- Security violation monitoring reports
- Vulnerability scanning plans
- Network penetration testing policy and procedure
- List of all user accounts with access to EPHI systems
- Configuration standards to include patch management for EPHI systems
- Encryption or equivalent measures implemented on EPHI systems

ecfirst

It's About 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*

2012 and beyond – it is about PII

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

ecfirst

Checklist for Breach Notification

Addressing Federal & State Mandates

1. Develop policy on Discovery, Reporting & Notification of Information Breaches
2. Review, update and integrate security controls and reporting capabilities for incident management
3. Create specific procedures for information breach management
4. Develop specific procedures for information breach notification
5. Conduct training for all members of the workforce

Incident Response for Breaches of PII
What is Your Formal Plan?

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

ecfirst

Contingency Planning

Exceptional Reference: NIST SP 800-34 Rev 1

1. Develop a Contingency Planning Policy
2. **Conduct Business Impact Analysis (BIA)**
   - *When did you conduct and complete a BIA exercise?*
3. Identify preventive 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
Most not in compliance

Encryption

Exceptional Reference: NIST SP 800-111

1. Develop comprehensive policy and conduct training
2. Consider solutions that use existing capabilities
3. Securely store and manage all keys
4. Select appropriate authenticators
5. Implement additional controls as needed

Confidential data at rest is a significant risk to organizations!

It Starts with Strategy

"The true organization is so prepared for battle that battle has been rendered unnecessary."

"Much strategy prevails over little strategy, so those with no strategy cannot but be defeated (defenses penetrated). Victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win."

Sun Tzu

The Art of War

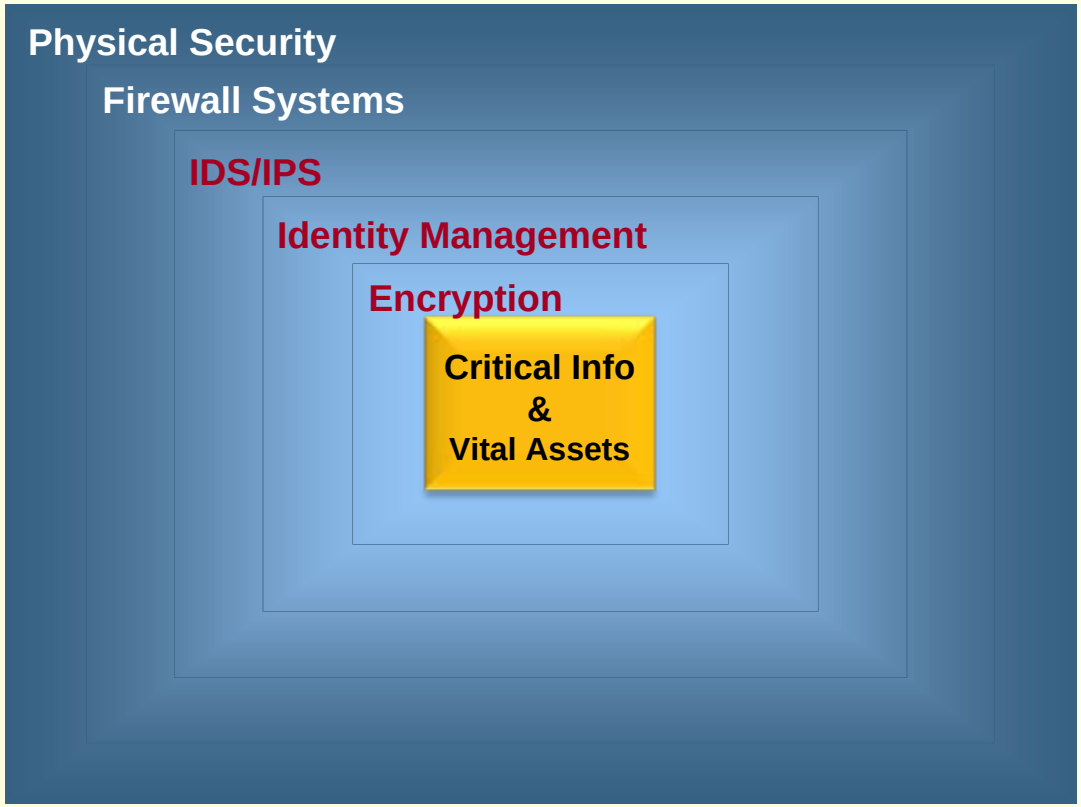
Critical for information security officers to seriously develop their strategy first, then execute.

Is your System Security Plan for 2012 Approved?

ecfirst

Information Security Program Strategy

Think 2012: ***Think Active Security***



Beyond Infrastructure Security.

Focus on Data Security.

ecfirst

Compliance & Security Priorities *In 2012*

- Conduct a formal risk analysis to establish baseline
  - A HITECH Meaningful Use Mandate!
- Schedule Regular Scans of the Infrastructure
  - Technical Vulnerability Assessment
- Develop a System Security Plan
- Use Corrective Action Plan (CAP) to Prioritize and Budget
- Update Security Policies
- Develop Contingency Plans (e.g. Disaster Recovery Plan)
- Implement Security Controls
  - Deploy Encryption Across Laptops, Backups, Removable Media
  - Deploy Single Sign-On (SSO) Solution
  - Activate Auditing Capabilities to Manage/Track Access
- Conduct Security Training & Awareness

Questions?

Free PDF! Checklist for HIPAA & HITECH Compliance.

Pabrai@ecfirst.com

ecfirst

About ecfirst

Health IT, Compliance & Security

Over 1,600 Clients served including **Microsoft, Cerner, HP, PNC Bank & hundreds of hospitals, government agencies**

ecfirst

Ali Pabrai, MSEE, CISSP (ISSAP, ISSMP)

Follow ecfirst for Daily Tips

Healthcare Information Security & Compliance Expert

- Created bizSHIELD™ – *an ecfirst Signature Methodology* - to address compliance and information security priorities
- Featured speaker at compliance and security conferences worldwide
- Presented at Microsoft, Intuit, Kaiser, E&Y, Federal & State Government agencies & many others
- Consults extensively with healthcare organizations, government agencies and business associates
- Established the HIPAA Academy and CSCS Program– gold standard for HIPAA, HITECH compliance solutions
- Member InfraGard
- Daily Compliance Tips: www.facebook.com/ecfirst

Like ecfirst on

ecfirst