

New! Checklist for HIPAA & HITECH Compliance

Pabrai

New! Checklist for HIPAA & HITECH Compliance

Ensure An Always Ready Audit State

The Sixth HIPAA Summit West
Healthcare Privacy and Security After HITECH and Health Reform



Ali Pabrai, MSEE, CISSP (ISSAP, ISSMP)

ecfirst, chief executive

Member, FBI InfraGard



Agenda

- Step through compliance challenges and state of security in healthcare
- Review list of critical security controls and associated skills – beyond policies, beyond training!
- Examine a checklist for ensuring compliance on a continual basis

Targeted attacks rose to average of 151/day in the first half of 2012 (Symantec Report).
WSJ, July 19, 2012

The Sixth HIPAA Summit West
Healthcare Privacy and Security After HITECH and Health Reform



New! Checklist for HIPAA & HITECH Compliance

Pabrai

State of Security

Risk to Information is a Risk to Business

“Cyber threat to our nation is one of the *most serious* economic and national security challenge we face.”
President Obama, WSJ, July 20, 2012

The Sixth HIPAA Summit West
Healthcare Privacy and Security After HITECH and Health Reform

Security Controls Implemented

Case Study: Client, May 8, 2012

Key Security Controls	
Implemented	Missing
Firewall (<i>Sonic Firewall TZ210</i>)	Two-factor authentication
IDS (<i>Dell SecureWorks</i>)	Data loss prevention solution
Antivirus protection (<i>Webroot</i>)	Security information/ and event manager
Data transfer (<i>SFTP, HTTPS</i>)	USB encryption
Remote access (<i>VPN, Citrix</i>)	Mobile device management
Asset management (<i>Dell KACE</i>)	
Laptop encryption (<i>TrueCrypt at the Bios Level; Windows OS & File Vault on Mac OS</i>)	
Email encryption (<i>Voltage</i>)	

The Sixth HIPAA Summit West
Healthcare Privacy and Security After HITECH and Health Reform

Compliance Grade

Risk Assessment Report Card

HIPAA Assessment Sections	Grade
Policies	C
Training	C
Controls	B
Skills	B+
Technical Vulnerabilities	Unknown
Executive Priority	B
Data Center	A
Overall Compliance Grade	B-

The Sixth HIPAA Summit West
Healthcare Privacy and Security After HITECH and Health Reform

Security Controls & Skills

- IDS/IPS**
 - Source Fire IPS, Cisco IPS, Checkpoint IPS, IBM Proventia
- SEIM**
 - ArcSight, LogRhythm, Splunk, LogLogic, McAfee Enterprise Security manager and Symantec Security Manager
- Vulnerability Scanners**
 - Qualys, Nexxpose Enterprise, nCircle 360, Nessus Professional

State of Security Controls

- What are your security controls?
- Who is actively managing the controls?

The Sixth HIPAA Summit West
Healthcare Privacy and Security After HITECH and Health Reform

BCBST Incident: Fast Facts

Understanding the Problem

OCR's first HITECH enforcement action related to a breach

- What Happened: 57 unencrypted hard drives stolen from a leased facility (discovered on October 5, 2009)
- # of Individuals Impacted: Contained EPHI of 1,023,209 individuals
- Perform monitor reviews to ensure compliance with CAP:
 - **Unannounced site visits** to facilities housing portable devices
 - Interviews with **random selection of 25 workforce members** who use portable devices
 - Review **use, retention, destruction of portable devices / e-media**
 - Inspection of **random sample of 25 portable devices** that contain EPHI to ensure compliance with policies

Data Breach:

400 entities reported breaches of 500 or more (OCR)

The Sixth HIPAA Summit West
Healthcare Privacy and Security After HITECH and Health Reform



Alaska DHSS: Fined \$1.7 M

How Prepared is Your Organization?

OCR's first HIPAA enforcement action for a State Agency

- Alaska DHSS: A portable electronic storage device (USB hard drive) possibly containing EPHI was stolen from vehicle of a DHSS employee
- **DHSS had not:**
 - Completed a risk analysis
 - Implemented sufficient risk management measures
 - Completed security training for its workforce members
 - Implemented device and media controls
 - Addressed device and media encryption

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

The Sixth HIPAA Summit West
Healthcare Privacy and Security After HITECH and Health Reform



Security Weaknesses

Areas of Concern

▪ Examples of weaknesses typically identified in providers:

- 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

➤ Breaches impact 19 million patients (OCR)

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

The Sixth HIPAA Summit West
Healthcare Privacy and Security After HITECH and Health Reform



Health IT Challenges

▪ Healthcare – Complex Computing Environment

- Cloud computing
- Virtualization
 - Servers
 - Desktop
- Mobile devices
- TBs of data across several storage media
- BYOD

▪ 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

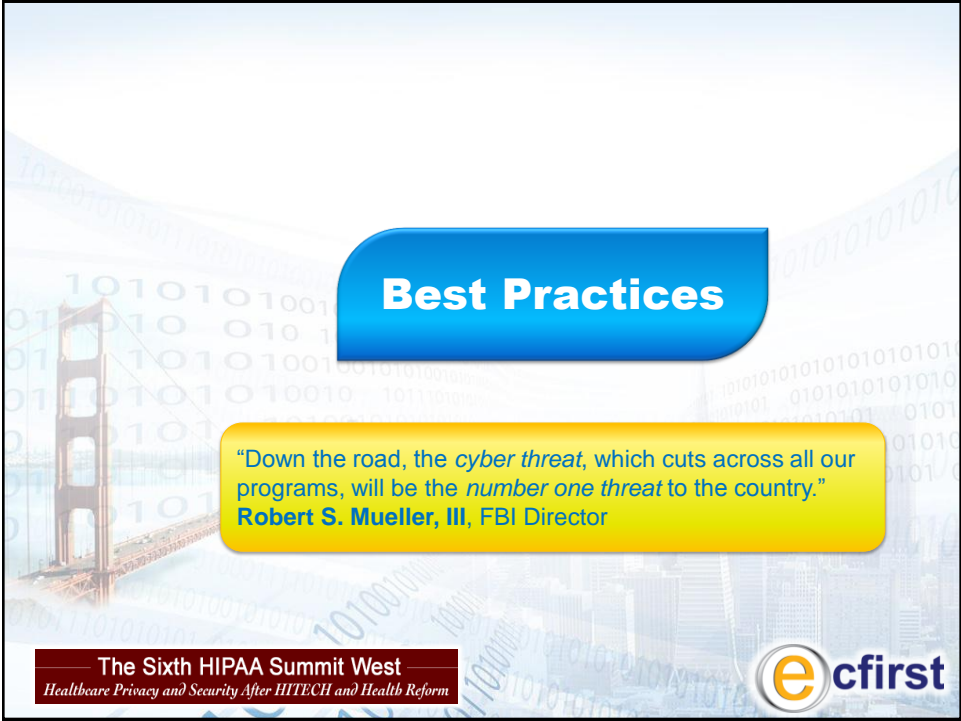
Risk to PII is a Risk to the Organization!

The Sixth HIPAA Summit West
Healthcare Privacy and Security After HITECH and Health Reform



New! Checklist for HIPAA & HITECH Compliance


Pabrai



Best Practices

"Down the road, the *cyber threat*, which cuts across all our programs, will be the *number one threat* to the country."
Robert S. Mueller, III, FBI Director

The Sixth HIPAA Summit West
Healthcare Privacy and Security After HITECH and Health Reform



A 7-Step Checklist!

Establish a Security Program!

The Seven Steps to Enterprise Security™



- 1 Security Responsibility
- 2 Risk Analysis
- 3 Security Strategy & Policies
- 4 Remediate
- 5 Secure Third Parties
- 6 Training
- 7 Evaluate

b i z S H I E L D™

The Sixth HIPAA Summit West
Healthcare Privacy and Security After HITECH and Health Reform



Risk Assessment & Treatment

- **Compliance or security gaps identified during a risk assessment may be managed by:**
 - A. Applying appropriate controls to reduce the risks
 - B. Knowingly and objectively accepting risks, providing they clearly satisfy the organization's policy and criteria for risk acceptance
 - C. Avoiding risks by not allowing actions that would cause the risks to occur
 - D. Transferring the associated risks to other parties, e.g., insurance or suppliers

The Sixth HIPAA Summit West
Healthcare Privacy and Security After HITECH and Health Reform



Security Policy

- Establishes the “dial-tone” for security in the organization
- Critical elements include:
 - ✓ Establishing management direction for information security
 - ✓ Regular updates and reviews
- Objective is to provide management direction & support for security in accordance with business requirements & relevant laws
- Policies should be approved by management, & published and communicated to all employees and relevant external parties
- NIST SP 800-53 establishes enterprise policy & procedure requirements
- PCI DSS Control Objective #6 (Requirement #12) is about maintaining information security policies

NIST SP 800-53: All XX-1 Controls

The Sixth HIPAA Summit West
Healthcare Privacy and Security After HITECH and Health Reform



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 Critical Requirement

The Sixth HIPAA Summit West
Healthcare Privacy and Security After HITECH and Health Reform



Encryption. Encryption. Encryption!

1. Develop an encryption policy
2. Establish standards for encryption across data @ rest & data in motion
3. Ensure enforcement of policy & standards across enterprise
4. Implement additional controls as needed

Confidential data at rest is a significant risk to organizations!

The Sixth HIPAA Summit West
Healthcare Privacy and Security After HITECH and Health Reform



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 2012-13 Approved?

The Sixth HIPAA Summit West
Healthcare Privacy and Security After HITECH and Health Reform



State of Security: Exec Dashboard

Hospital Somewhere

HIPAA & HITECH Risk Analysis Report

bizSHIELD

March 1st, 2011


HITECH Meaningful Use / EHR Mandate

Core Objective	Meaningful Use/EHR Objective	Measurement
#15	Implement systems to protect privacy and security of patient data.	Conduct or review a security risk analysis and implement security updates as necessary, and correct identified security deficiencies.

HIPAA / HITECH Report Card

HIPAA Mandate	Overall Report 2010
Policies	Need to not out & provide training
Training	Below Average
Controls	Below Average
Skills	Good
Technical Vulnerabilities	Average
Executive Priority	Below Average
Data Center	Average
Overall Compliance Grade	D+

Overall Compliance



164.308(a)(1)(ii)(A) Risk Analysis (Required). Conduct accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

Compliance Status

2010	Exceeded		Met		Implementation Specifications	
	Total	Compliant	Non-Compliant	Total	Compliant	Partially Compliant
Administrative	5	0	9	20	1	12
Physical	4	0	4	8	1	4
Technical	5	0	5	7	0	5
Organizational	2	1	1	2	1	1
Policies & Procedures	2	1	2	3	0	3
Totals	22	1	2	40	3	25

Corrective Action Plan

To be completed within 90 days of receipt of report

High

- Appoint a Compliance, Privacy & Security Officer
- Build HIPAA Center of Expertise & Dedication To Compliance
- Develop Organization Policies & Procedures
- Identify All EPHI Within the Organization
- Informal System Activity Review
- Implement a Formal Password Policy
- Consistent Security Controls
- Logging and Log Monitoring

Medium

- Implement a Change Management Process
- Implement Disk Encryption
- Business Continuity Planning & Disaster Recovery
- Create a Workstation Logout & Auto Lock Policy
- Create a Security Road Map
- Create a Mobile Media Policy & Procedures Document
- Provide Security Reminders to Employees
- Implement an Incident Management Program

To be completed within 180 days of receipt of report


High

- Assess Budget Requirements for Data Loss Prevention
- Ensure all Firewall Rules are Tied to Business Needs
- Applications to use RBAC
- Discontinue use of Insecure Protocols
- Document in Writing & Store Copies in Multiple Locations of all Backup & Restore Procedures for all Information Systems & Infrastructure Devices.
- Implement User Audits

Medium

- Discontinue use of Insecure Protocols
- Secure Guest Wireless Access Point
- Enable Rogue AP Detection on the Wireless Network
- Staffing Ratios
- Develop a Project Plan to Identify & Quantify the use of Portable Media Devices across the Enterprise

The Sixth HIPAA Summit West
Healthcare Privacy and Security After HITECH and Health Reform



2012. All Rights Reserved. ecfirst.

9

Questions?
Questions?

Are we excited?

ecfirst
Compliance & Security

Industry leader delivering world-class services in Compliance & Information Security for over a decade

Recognized as an Inc. 500 Business in 1st year of eligibility

Minority Business Enterprise Certified

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

Over 1,600 Clients served including Microsoft, Cerner, HP, State of Utah, PNC Bank & hundreds of hospitals, government agencies, business associates

New! Checklist for HIPAA & HITECH Compliance

Pabrai

Ali Pabrai, MSEE, CISSP (ISSAP, ISSMP)

Follow *ecfirst* for Daily Tips  

Information Security & Compliance Expert

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



Did you get information of value from this brief?
"Like" *ecfirst* on 