Firewalls to Encryption
Compliance Mandates and Cyber Security

THE TWENTY-FIRST NATIONAL **HIPAA SUMMIT**

The Leading Forum on Healthcare EDI, Privacy, Confidentiality, Data Security and HIPAA Compliance

Ali Pabrai, MSEE, CISSP (ISSAP, ISSMP)

ecfirst, chief executive

ecfirst

Agenda

- Human body: Specialized organs
- Security controls: A critical component for compliance
- HIPAA checklist: Ensuring compliance on a continual basis


Human Body:
Specialized Organs!
ecfirst


Human Body: Impact of What We Eat!
THE TWENTY-FIRST NATIONAL
HIPAA SUMMIT
The Leading Forum on Healthcare EDI, Privacy, Confidentiality, Data Security and HIPAA Compliance
ecfirst

Human Body: What We Eat!

Component	Description
Blueberries	Rich in antioxidants that help keep our cells healthy, improves memory & can reverse age-related decline in motor function, balance & coordination.
Broccoli	High in vitamin K & improves memory function, as well as slows the aging process.
Flaxseed	Packed with omega-3 fatty acids, that helps your brain function.
Wild salmon	Rich in omega-3 fatty acids & helps develop tissue for increasing your brainpower.
Egg yolks	Are rich in choline, a nutrient that improves memory & minimizes fatigue.
Legumes (beans)	Can raise alertness and stimulate nerve impulses in the brain.
Walnuts	Rich in omega-3 fatty acids, while almonds contain natural mood-enhancing neuro-transmitters.

What Security Controls Have Been Deployed?

"*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 TWENTY-FIRST NATIONAL **HIPAA SUMMIT** The Leading Forum on Healthcare EDI, Privacy, Confidentiality, Data Security and HIPAA Compliance

ecfirst

Firewalls: First Line of Defense!

- What are your firewall configuration standards?
  - Is there a formal process for approving and testing all external network connections and changes to the firewall configuration?
  - Does a current network diagram with all connections, including any wireless networks?
  - What are the requirements for a firewall at each Internet connection and between any Demilitarized Zone (DMZ) and the internal network zone?
  - Is there a documented list of services and ports necessary for business?
  - What is the justification and documentation for any risky protocols allowed (for example, FTP), which includes reason for use of protocol and security features implemented?
  - Is there a formal review of firewall and router rule sets? At what frequency? Who is responsible? Who is accountable?
  - What are your configuration standards for communication devices such as routers, switches, access points, and others?
- Key - disable all unnecessary and insecure services & protocols

Anti-Virus Control

- Many vulnerabilities and malicious viruses enter the network via employees' email activities
- Anti-virus software must be used on all systems commonly affected by viruses to protect systems from malicious software
- Deploy anti-virus software on all systems commonly affected by viruses (particularly end systems & servers)
- Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including spyware & adware
- Ensure that all anti-virus mechanisms are current, actively running, & capable of generating audit logs

Authentication Control

- Identify all users with a unique user name before allowing them to access systems with EPHI
- In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:
  - Strong Password
  - Token Devices (e.g., SecureID, certificates, or public key)
  - Biometrics
- Implement two-factor authentication for remote access
- Encrypt all passwords during transmission & storage on all system components

Audit Log Consolidation Control

- Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user
- Implement automated audit trails for all system components to reconstruct the following events:
  - All individual user accesses to EPHI
  - All actions taken with root or admin privileges
  - Access to all audit trails
  - Invalid logical access attempts
  - Use of identification & authentication mechanisms
  - Initialization of the audit logs
  - Creation and deletion of system-level objects

Audit Log Consolidation Control

- Secure audit trails so they cannot be altered
  - Limit viewing of audit trails to those with a job-related need
  - Protect audit trail files from unauthorized modifications
  - Promptly back-up audit trail files to a centralized log server or media that is difficult to alter
  - Copy logs for wireless networks onto a log server
  - Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts
- Review logs for all system components at least daily
- Retain audit trail history for at least one year, with a minimum of three months online availability

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!

Encryption Control

- Protect encryption keys used for encryption against both disclosure and misuse
  - Restrict access to keys to the fewest number of custodians necessary
  - Store keys securely in the fewest possible locations and forms
- Fully document and implement all key management processes and procedures for keys used for encryption, including the following:
  - Generate strong keys
  - Secure key distribution
  - Secure key storage
  - Periodically change keys

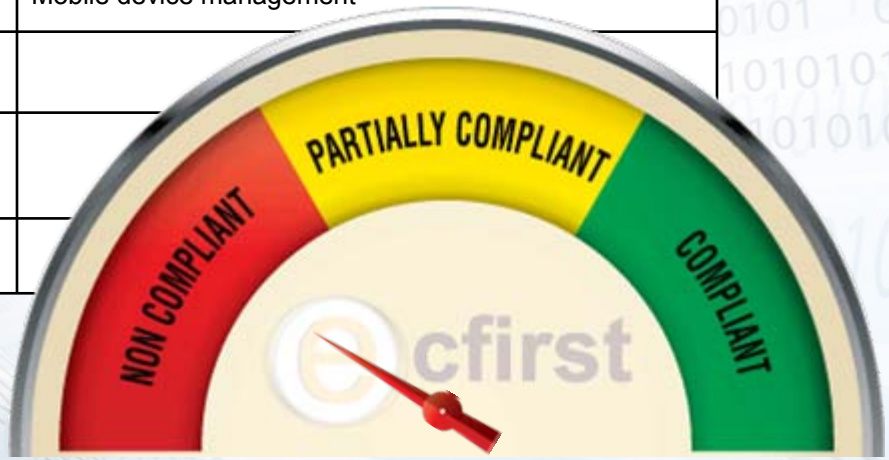
Encryption Control

- At least annually
  - Destroy old keys
  - Split knowledge and establishment of dual control of keys
  - Prevent unauthorized substitution of keys
  - Replace known or suspected compromised keys
  - Revoke old or invalid keys
  - Require key custodians to sign a form stating that they understand & accept their key-custodian responsibilities
- Use strong cryptography & security protocols such as SSL/TLS and IPSEC to safeguard sensitive during transmission over open, public networks
- Never send unencrypted EPHI by email or other applications (texting)

Security Controls Implemented

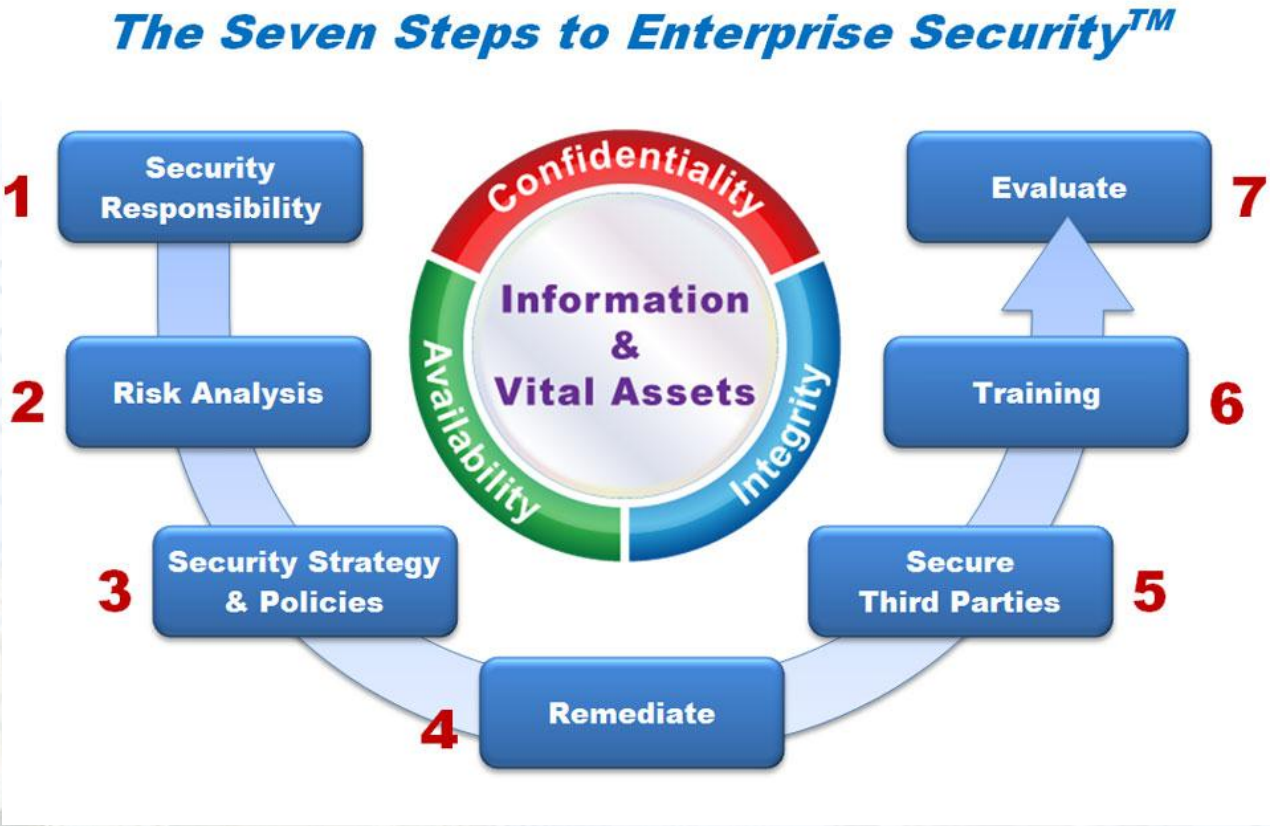
Case Study: Client, December 12, 2012

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



HIPAA Checklist!

Establish an Enterprise Program!



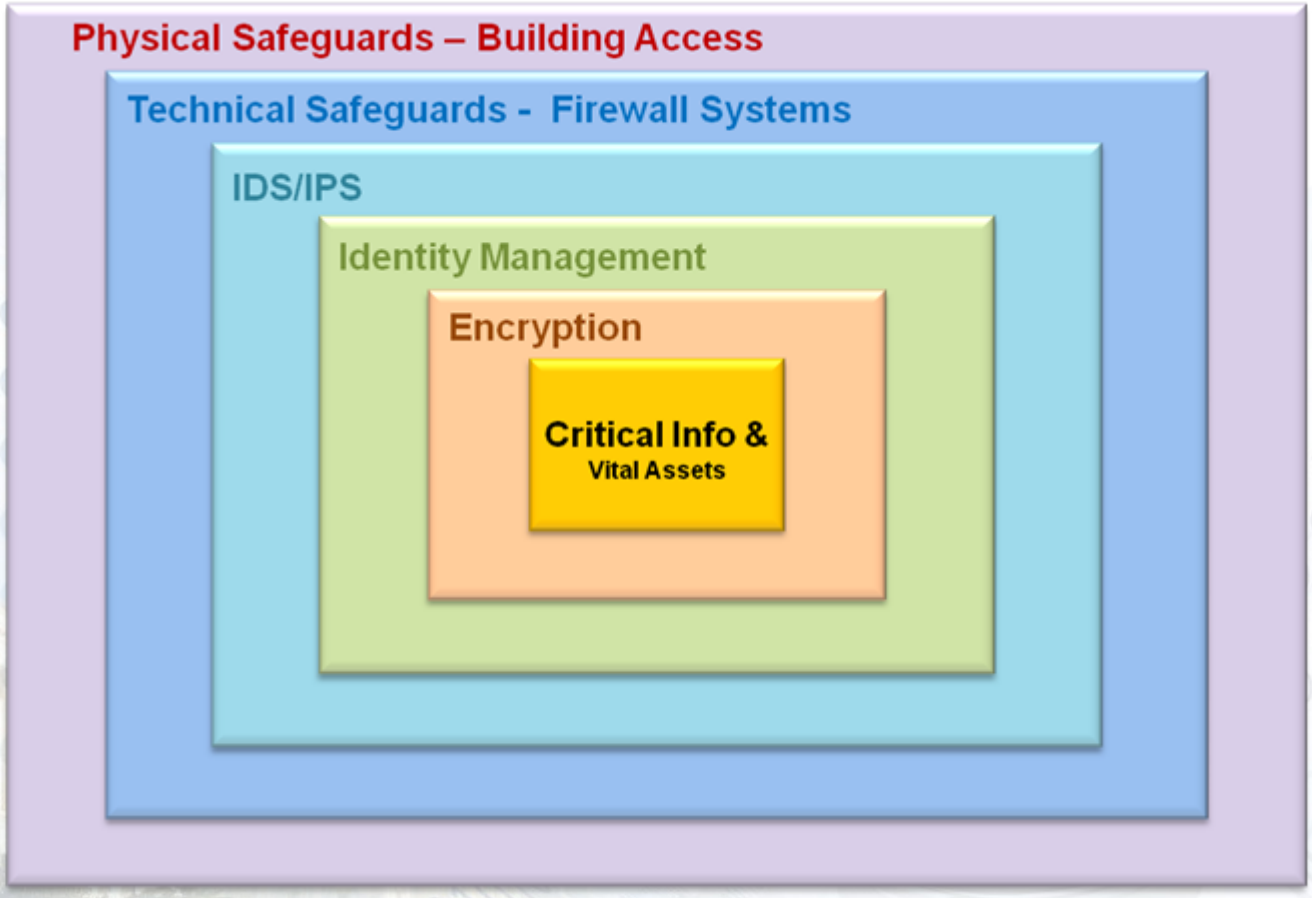
bizSHIELD tm

THE TWENTY-FIRST NATIONAL HIPAA SUMMIT The Leading Forum on Healthcare EDI, Privacy, Confidentiality, Data Security and HIPAA Compliance

ecfirst

Information Security Strategy

Core to the Edge & the Cloud



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

Pabrai's Laws of Information Security

Is Your Security Kismet or Karma?

1. There is no such thing as a 100% secure environment
2. Security is only as strong as your weakest link
3. Security defenses must be integrated and include *robust* (passive) and *roving* (active) controls to ensure a *resilient* enterprise
4. Security *incidents* provide the foundation for security *intelligence*

Is Your HIPAA Compliance Program?

Kismet – A Reactive Security Framework

Karma – A Proactive Security Framework

"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

Questions?

Are we excited?

ecfirst

ecfirst

Compliance & Security

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

ecfirst

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 *biz*SHIELD^{tm} – *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

ecfirst