



THE TWENTY-THIRD NATIONAL HIPAA SUMMIT

**Compliance & Cyber Security:
Enabling a Credible Program**
March 17, 2015 Washington, DC

ecfirst



About Your Presenter

THE TWENTY-THIRD NATIONAL HIPAA SUMMIT

Ali Pabrai
MSEE, CISSP (ISSAP, ISSMP)

Information Security & Compliance Expert

- Consults extensively with technology firms, government agencies and business associates
- Created *bizSHIELD*[™] – a Signature Methodology - to address compliance & information security priorities
- Featured speaker at InfoSec conferences worldwide
- Presented at Microsoft, Kaiser, Intuit, E&Y, Federal & State Government agencies & many others
- Established the HIPAA Academy & CSCS Programs – gold standard for cyber security & compliance solutions
- Interim CISO for large health system with 30+ locations across the USA
- Member InfraGard (FBI)
- www.facebook.com/ecfirst & www.facebook.com/Pabrai.

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

ecfirst

Agenda

THE
TWENTY-THIRD
NATIONAL
HIPAA SUMMIT

- **Cyber Risk = Business Risk**
 - Breaches: banks, retailers, healthcare
 - Cyber attack lifecycle
 - Anatomy of an attack
- **Compliance Mandates**
 - ISO 27000, PCI DSS, NIST & More
- **Security Controls**
 - Firewalls to Encryption
 - Importance of Technical Vulnerability Assessments
- **Your Enterprise Security Plan**
 - A Checklist
- **December 31, 2015**

Taoguang yanghui, is a Chinese saying, “hiding capabilities & bidding one’s time”



Anthem's Massive Data Breach *About 80 M Customers & Employees Impacted*

THE
TWENTY-THIRD
NATIONAL
HIPAA SUMMIT

Bottom-line Facts:

- Attackers gained unauthorized access to Anthem's database systems & obtained PII
- Suspicious activity was first noticed on Jan 27, 2015 and seemed to show unauthorized activity to the vast database since Dec 10, 2014
- Discovery of information includes IP addresses & email addresses believed to be associated with the threat actors
- Information compromised included PII on former & current employees (names, birthdays, medical IDs, SS #'s, street addresses, email addresses, employment data, including income data); not known if healthcare or financial data was stolen; records as far back as 2004 may have been compromised
- The database was not encrypted
- 9 days after breach reported, Anthem offered victims 2 years of free credit monitoring, ID theft insurance, & identity repair monitoring
- The good news, if there is one, is that Anthem discovered the breach itself & was quick in incident response



Anthem's Massive Data Breach

THE
TWENTY-THIRD
NATIONAL
HIPAA SUMMIT

- *How was the breach discovered?* An Anthem IT System Administrator noticed that a database query was being run using his identifier code although he had not initiated it
- The Anthem attack seems to have relied on malware & tools used by Chinese hackers
- The hackers used a stolen employee password to access the database
- *What now?* Passwords have been reset for all employees with privileged access to database systems
- Also, access has been blocked to any access that requires only one password to such sensitive systems
- **Note:** in 2013, Wellpoint (now called Anthem) settled with OCR for \$1.7 M due to improper EPHI safeguards; unauthorized access was allowed through its online health insurance portal (*testing was inadequate & not checked to see modifications performed as intended*)



Breach History & Fine with Wellpoint

THE
TWENTY-THIRD
NATIONAL
HIPAA SUMMIT

- Wellpoint did not adequately implement policies & procedures for authorizing access to EPHI of its web-based application database
- Wellpoint did not perform an adequate technical evaluation in response to a software upgrade, an operational change affecting the security of EPHI maintained in its web-based application database that would establish the extent to which the configuration of the software providing authentication safeguards for its web-based application met HIPAA requirements
- WellPoint did not adequately implement technology to verify that a person or entity seeking access to EPHI maintained in its web-based application database is the one claimed
- Between October 23, 2009, until March 7, 2010, WellPoint impermissibly disclosed the EPHI, including the names, dates of birth, addresses, SS #, telephone numbers & health information, of approximately 612,000 individuals whose EPHI was maintained in the web-based application database
- Wellpoint fined \$1.7 M by OCR/HHS on July 11, 2013



Iran Cyber Attacks

THE
TWENTY-THIRD
NATIONAL
HIPAA SUMMIT

Learning from Iran Cyber Attacks

- Attack identified on December 2, 2014
 - More than 50 targets in 16 countries
- Used common SQL injection, spear phishing & other attacks to gain initial access to one or more computers of targeted organization
- Next, used privilege escalation exploits & other tools to compromise additional systems & move deeper inside the compromised firm



Sony Cyber Attack

THE
TWENTY-THIRD
NATIONAL
HIPAA SUMMIT

Learning from Sony Cyber Attack

- Attack disclosed on Nov 24, 2014, when Sony workers received an email from hackers with an image of a skeleton & text
- A group called Guardians of Peace (GOP) said to be behind the attack
 - “God’sApstls” found in the malware that was used to break into Sony’s computers & steal data
 - Erased 1000’s of sensitive documents from hard drives
- GOP used highly sophisticated malware to carry out the attack
- The “wiper” malware attack has numerous commonalities with previous attacks in Saudi Arabia & South Korea

Hackers exposed private information about employees as well as celebrities associated with Sony

Hackers devastated Sony’s computer networks.



Bank Breach

THE
TWENTY-THIRD
NATIONAL
HIPAA SUMMIT

Learning from Chase Cyber Attacks

Bottom-line Facts:

- Attacks started in June 2014
- Breach detected as a result of a routine scan
- Hackers compromised flaw in bank web-site
- Hackers reached deep into enterprise infrastructure
- Gigabytes of customer account and other data siphoned slowly
- Attack routed through several countries, including Brazil, and then re-directed to Russia
- Layers of malware from Russia (likely) installed on compromised systems

Your capabilities to actively monitor critical systems?



CHS Breach

THE
TWENTY-THIRD
NATIONAL
HIPAA SUMMIT

Learning from Community Health Systems (CHS)

Bottom-line Facts:

- On August 18, 2014 announced breach impacting 4.5 million patients
- Attacks occurred from April 2014 to June 2014
- Breach detected July 2014
- Attacker used HeartBleed to retrieve content of Juniper device memory
- Juniper device HeartBleed vulnerability exploited by attackers to gain access to valid user credentials
- User credentials used to login to CHS internal network via a VPN

How robust is your patch management?



Breaches @ Retailers

THE
TWENTY-THIRD
NATIONAL
HIPAA SUMMIT

- POS malware compromises cash registers that monitor card authorization process
- RAM-scraping malware steals unencrypted data from memory
- Stolen information copied to a compromised internal system & transmitted outside
- Before a transaction can be authorized, card data is momentarily decrypted & stored in memory (RAM)

Breach was deeper than previously reported

Hackers invaded systems for several months



Coke Compromised

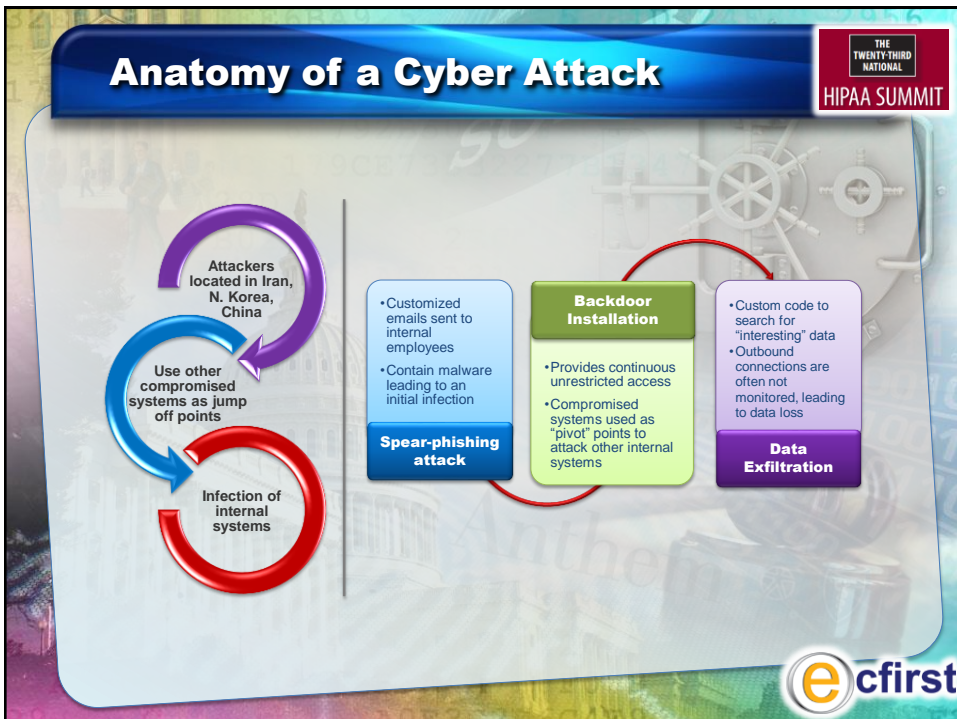
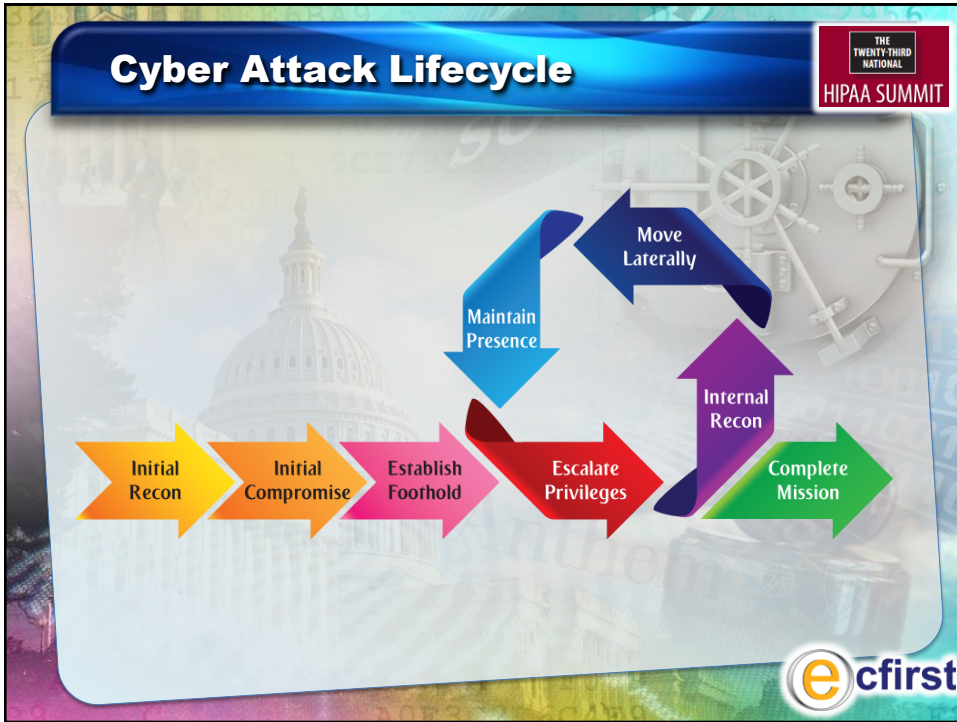
THE
TWENTY-THIRD
NATIONAL
HIPAA SUMMIT

The New York Times

- PII on 70,000 workforce members compromised (including contractors, vendors)
- Data not encrypted stolen by a former worker responsible for maintaining & disposing of company equipment
- Breach discovered Dec 10, 2013
- Breach disclosed Jan 23, 2014
- Stolen computers belonged to employees who worked in HR & had access to HR records

Insider threats must be within scope of risk analysis







Compliance Mandates

THE TWENTY-THIRD NATIONAL HIPAA SUMMIT

The image shows three classical pillars on the left, each with a red label: CONFIDENTIALITY, INTEGRITY, and AVAILABILITY. To the right are three colored circles representing standards: a red circle for ISO 27000, a blue circle for PCI DSS, and a green circle for NIST. The background features a faint image of a classical building and a ship's wheel.

ISO 27000 Updates

THE TWENTY-THIRD NATIONAL HIPAA SUMMIT

ISO 27002: 2005	ISO 27002: 2013
Security Policy	Information Security Policies
Organizing Information Security	Organization of Information Security
Asset Management	Human Resource Security
Human Resources Security	Asset Management
Physical & Environmental Security	Access Control
Communications & Operations Management	Cryptography
Access Control	Physical & Environmental Security
Information Systems Acquisition, Development & Maintenance	Operations Security
Information Security Incident Management	Communications Security
Business Continuity Management	System Acquisition, Development & Maintenance
Compliance	Supplier Relationships
	Information Security Incident Management
	Information Security Aspects of Business Continuity Management
	Compliance

PCI DSS Requirement 12.2

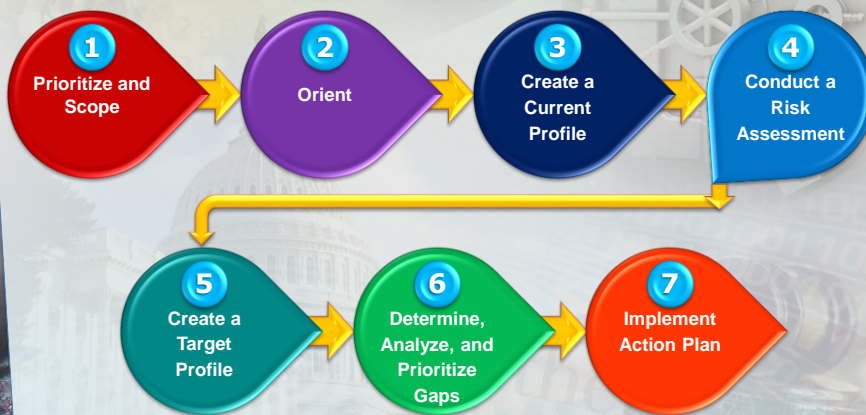
THE TWENTY-THIRD NATIONAL HIPAA SUMMIT

PCI DSS Requirements	Testing Procedures
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	12.1 Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners).
12.1.1 Addresses all PCI DSS requirements.	12.1.1 Verify that the policy addresses all PCI DSS requirements.
12.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment. (Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 & NIST SP 800-30).	<p>12.2.a Verify that an annual risk assessment process is documented that identifies threats, vulnerabilities, and results in a formal risk assessment.</p> <p>12.2.b Review risk assessment documentation to verify that the risk assessment process is performed at least annually & upon significant changes.</p>



NIST: Cyber Security Program

THE TWENTY-THIRD NATIONAL HIPAA SUMMIT



THE TWENTY-THIRD NATIONAL HIPAA SUMMIT

Security Controls

“Cyber threat to our nation is one of the most serious economic and national security challenge we face.”
President Obama

ecfirst

THE TWENTY-THIRD NATIONAL HIPAA SUMMIT

Security Controls

Key Security Controls	
Implemented	Missing
Firewall (<i>Sonic Firewall TZ210</i>)	Two-factor authentication
IDS (<i>Dell SecureWorks</i>)	DLP
Antivirus protection (<i>Webroot</i>)	Secure text messaging
Data transfer (<i>SFTP, HTTPS</i>)	USB & portable device encryption
Remote access (<i>VPN, Citrix</i>)	MDM
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>)	

ecfirst

Implementing Security Controls

THE
TWENTY-THIRD
NATIONAL
HIPAA SUMMIT

- **Firewall/DMZ:** Disable all unnecessary and insecure
- **Anti-Virus:** Ensure that all anti-virus mechanisms are current, actively running, & capable of generating audit logs
- **Logs:** Review logs for all system components at least daily
- **Audit History:** Retain audit trail history for at least one year, with a minimum of three months online availability



Encryption!

THE
TWENTY-THIRD
NATIONAL
HIPAA SUMMIT

Partial Checklist	STATUS	
	YES	NO
Has your organization implemented encryption for EPHI/PII transmission?	<input type="checkbox"/>	<input type="checkbox"/>
How has the organization addressed protecting EPHI/PII for data at rest?	<input type="checkbox"/>	<input type="checkbox"/>
Is encryption feasible & cost-effective for your organization?	<input type="checkbox"/>	<input type="checkbox"/>
What encryption systems & technologies does your organization use?	<input type="checkbox"/>	<input type="checkbox"/>
Does your organization have staff skilled in the use of encryption?	<input type="checkbox"/>	<input type="checkbox"/>
Does the organization have a secure texting policy and associated capabilities implemented?	<input type="checkbox"/>	<input type="checkbox"/>
Has email encryption been implemented by the organization?	<input type="checkbox"/>	<input type="checkbox"/>



Encryption!

THE TWENTY-THIRD NATIONAL HIPAA SUMMIT

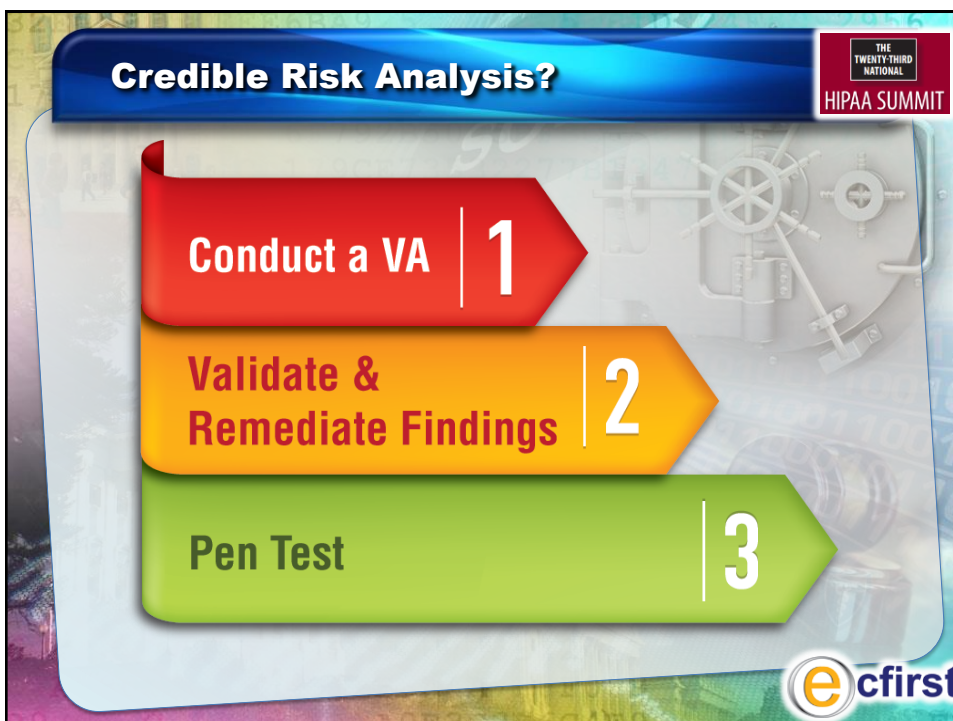
AREA	STATUS	
	YES	NO
Database Servers	<input type="checkbox"/>	<input type="checkbox"/>
PII/PHI on Cloud Systems	<input type="checkbox"/>	<input type="checkbox"/>
Backup Media	<input type="checkbox"/>	<input type="checkbox"/>
Desktops	<input type="checkbox"/>	<input type="checkbox"/>
Laptops	<input type="checkbox"/>	<input type="checkbox"/>
Tablets	<input type="checkbox"/>	<input type="checkbox"/>
Smart Phones	<input type="checkbox"/>	<input type="checkbox"/>
USB Devices	<input type="checkbox"/>	<input type="checkbox"/>
Email	<input type="checkbox"/>	<input type="checkbox"/>
Text Messages	<input type="checkbox"/>	<input type="checkbox"/>
Remote Access	<input type="checkbox"/>	<input type="checkbox"/>
Wireless	<input type="checkbox"/>	<input type="checkbox"/>
Transmission	<input type="checkbox"/>	<input type="checkbox"/>

ecfirst

THE TWENTY-THIRD NATIONAL HIPAA SUMMIT

Enterprise Security Plan

ecfirst



Discovering Vulnerabilities

THE TWENTY-THIRD NATIONAL HIPAA SUMMIT

External

Internal

Discovering Vulnerabilities

Firewall/DMZ

Wireless

Fine for Unpatched Software
\$150,000 fine with a 2-year Corrective Action Plan (CAP)

ecfirst

December 31, 2015?

THE TWENTY-THIRD NATIONAL HIPAA SUMMIT

What is the state of your enterprise security & compliance?

Cyber Risk = Business Risk

ecfirst

Questions?

Are we excited?

ecfirst

The HIPAA Portal
www.HIPAAAcademy.net/portal/

The HIPAA Portal

ecfirst

Cyber Security Portal

www.ecfirst.com/cyber



Cyber Security Portal
A cyber security knowledge portal.



ecfirst Compliance & Security



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

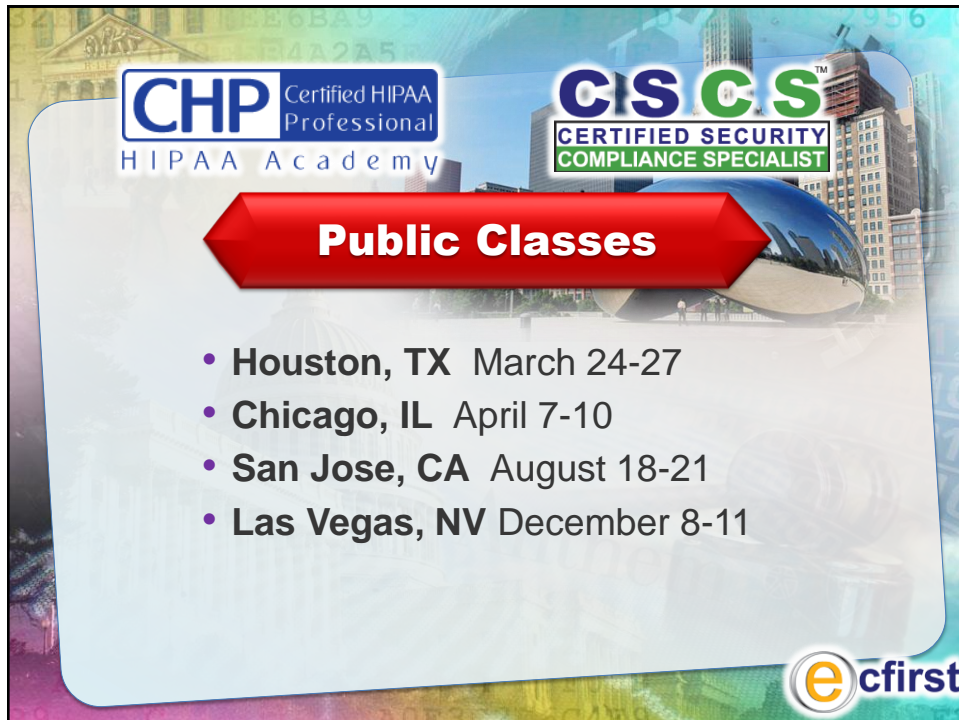
Recognized as an Inc. 500 Business in 1st year of eligibility

Minority Business Enterprise Certified

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

Over 2,100 clients served including Microsoft, Cerner, HP, State of Utah, PNC Bank, IBM, Kaiser & hundreds of hospitals, government agencies, business associates in India, Philippines





The slide features a background with a cityscape and a large, reflective sphere. In the top left, the logo for 'CHP Certified HIPAA Professional HIPAA Academy' is displayed. In the top right, the logo for 'CSCS CERTIFIED SECURITY COMPLIANCE SPECIALIST' is shown. A red arrow-shaped banner in the center contains the text 'Public Classes'. Below this banner is a bulleted list of four class locations and dates. The 'ecfirst' logo is in the bottom right corner.

CHP Certified HIPAA Professional
HIPAA Academy

CSCS™
CERTIFIED SECURITY
COMPLIANCE SPECIALIST

Public Classes

- **Houston, TX** March 24-27
- **Chicago, IL** April 7-10
- **San Jose, CA** August 18-21
- **Las Vegas, NV** December 8-11

ecfirst



The slide features a background with a cityscape and a large, reflective sphere. In the top center, the logo for 'CHP Certified HIPAA Professional HIPAA Academy' is displayed. Below the logo is a bulleted list of six topics. The 'ecfirst' logo is in the bottom right corner.

CHP Certified HIPAA Professional
HIPAA Academy

- **HIPAA, HITECH and the Omnibus Final Rule**
- **How the HITECH Act affects organizations with access to health information**
- **HIPAA Privacy and Security Rules**
- **HIPAA Transactions Code Sets and Identifiers**
- **Compliance challenges & best practices**
- **Plan and prepare for HIPAA compliance**

ecfirst



CSCSTM
**CERTIFIED SECURITY
COMPLIANCE SPECIALIST**

- HITECH & the HIPAA Security Rule
- FISMA, NERC CSS, & GLBA
- PCI DSS
- ISO 27001, ISO 27002, ISO 27799 & others
- Federal & State regulations
- NIST

ecfirst



ecfirst **HIPAA**TM
Academy

Thank You!

Pabrai@ecfirst.com
Cell: +1.949.528.5224

ecfirst