Wireless Security and the HIPAA Security Rule

HIPAA Academy™
HIPAAacademy.Net

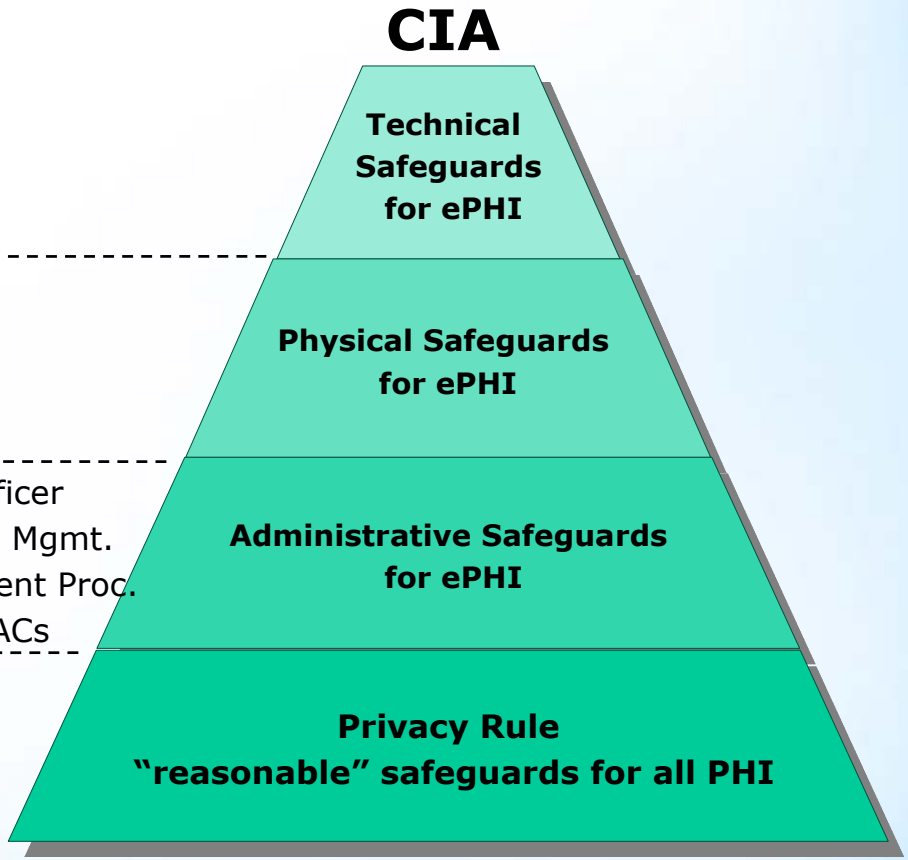
Uday O. **Ali** Pabrai, CISSP, CHSS

HIPAA Security Rule

- Access Control
- Audit Control
- Integrity
- Person or Entity Authentication
- Transmission Security

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device & Media Controls

- Security Mgmt. Process, Sec. Officer
- Workforce Security, Info. Access Mgmt.
- Security Training, Security Incident Proc.
- Contingency Plan, Evaluation, BACs



Transmission Security

- Standard requires covered entities to implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network
  - Integrity Controls (A)
  - Encryption (A)

Integrity Controls & Encryption

- Integrity Controls:
  - Implement security measures to make sure that electronically transmitted ePHI is not improperly modified without detection until disposed off properly
- Encryption:
  - Implement a mechanism to encrypt ePHI whenever deemed appropriate

Access and Audit Controls

- Access Control
  - Unique user identification (R)
  - Automatic logoff (A)
- Audit Controls
  - Record and examine activity

IEEE 802.11 Standards

- Many standards defined including:
  - 802.1x
  - 802.11a/b
  - 802.11e
  - 802.11f
  - 802.11i
  - 802.16a
  - 802.20

Wireless Network Components

- Wireless NIC
  - PC, USB or PCI cards
- Client system
- Communications medium
- Access point

- Operating modes
  - Ad-hoc or Infrastructure

Security Challenges

- **Lack of user authentication**
- **Weak encryption**
- **Poor network management**
- **Vulnerable to attacks:**
  - Man-in-the-middle
  - Rogue access points
  - Session hijacking
  - DoS

Security Protocols

- Wired Equivalent Privacy (WEP)
- IEEE 802.1x User Authentication
- Extensible Authentication Protocol (EAP)
- Wi-Fi Protected Access (WPA)

Getting Started

- **Conduct risk analysis**
- **Develop security policies**
  - Wireless
    - Mobile devices
  - Encryption
- **Remediation: Design infrastructure**
  - Firewall
  - IDS
  - Wired network

Approach: 7 Steps Roadmap

HIPAA Academy™
HIPAAacademy.Net

Step 2: Risk Analysis

- “99% of all reported intrusions result through exploitation of known vulnerabilities or configuration errors, for which safeguards and countermeasures are available”

NIST 2004

- “In 2003, the health care industry was subject to the third highest number of severe events”

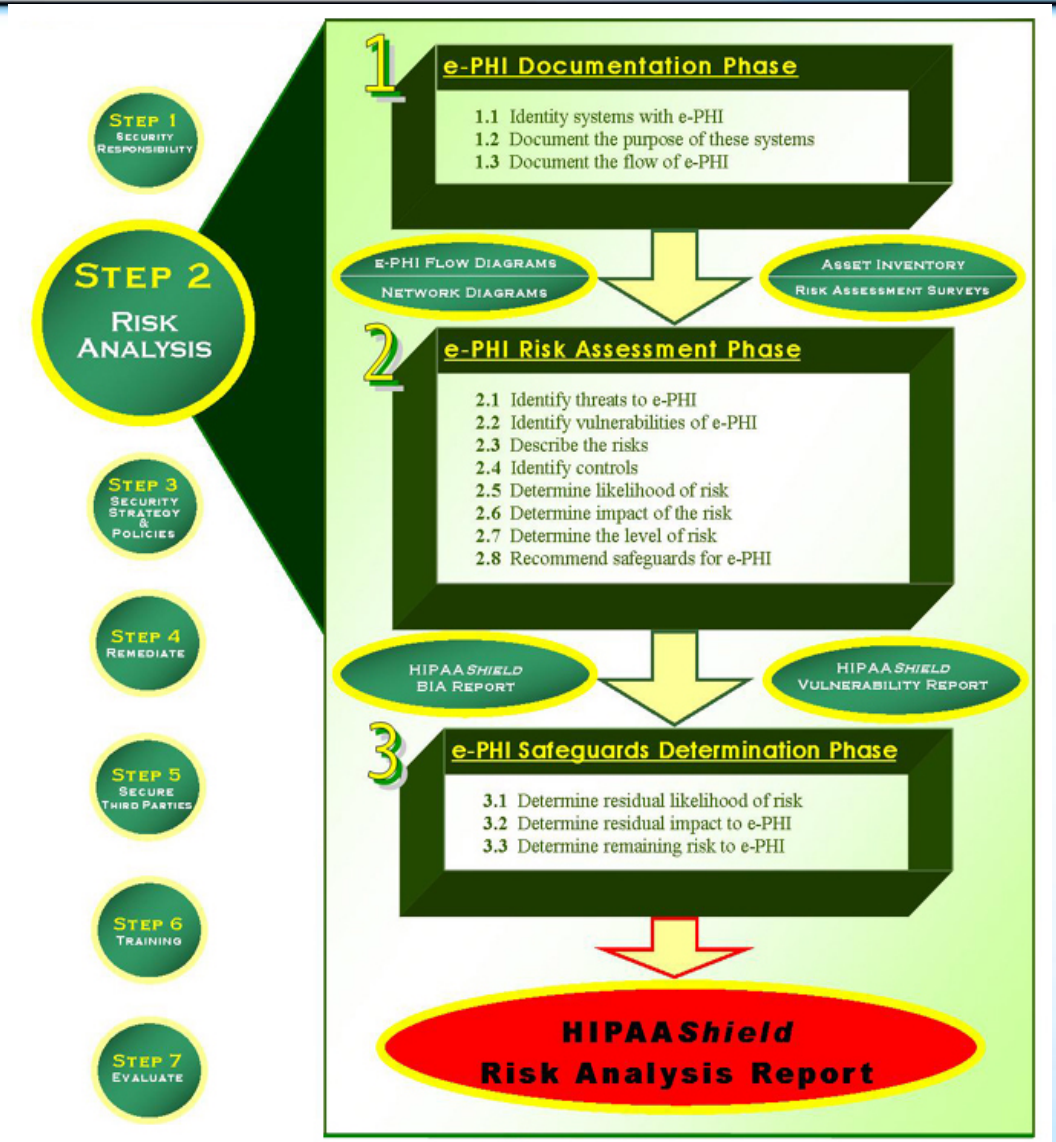
Symantec 2004

Step 2: Risk Analysis

- "Every covered entity must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of its electronic Protected Health Information (ePHI)"

HIPAA Security Rule

Step 2: Risk Analysis



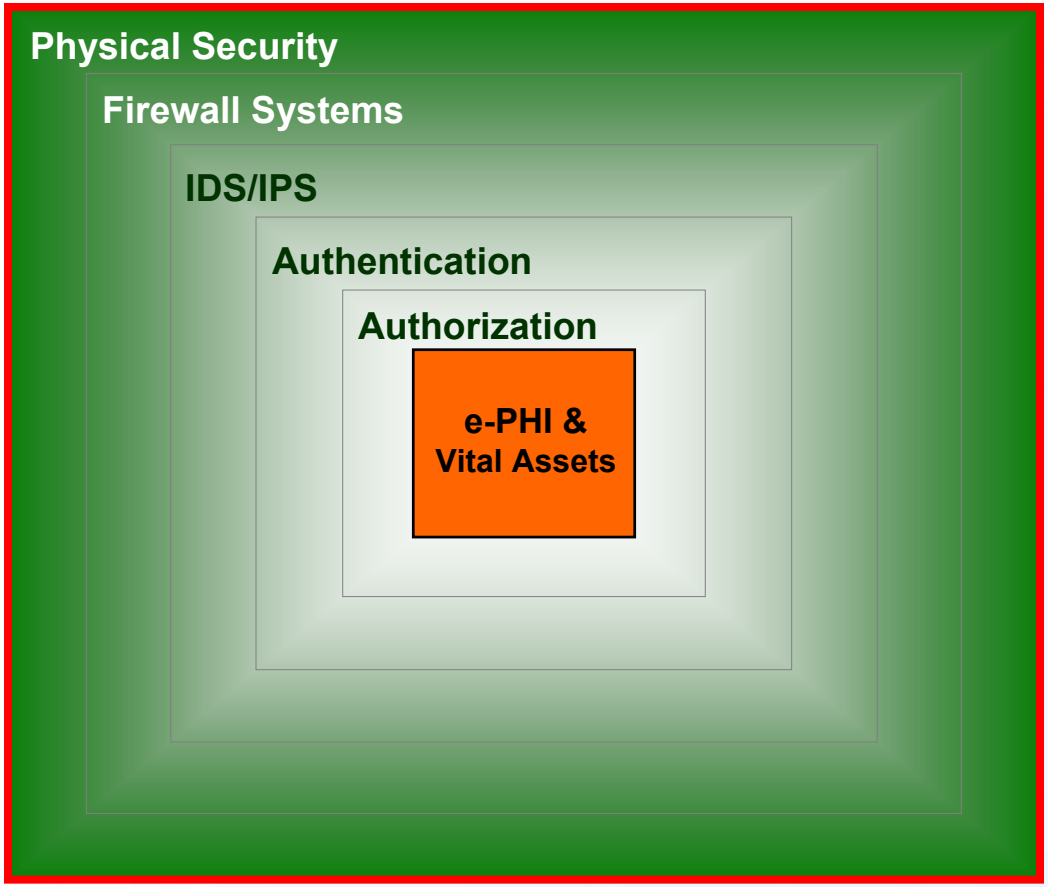
Wireless Security Policy

- **Define scope**
  - Transmission
  - Mobile devices
- **Establish guidelines for deployment**
  - 128-bit encryption
  - MAC address that is registered and tracked
  - Strong user authentication
    - Mobile devices must have strong passwords
  - Mobile devices must have auto-logoff, screen savers
    - Establish time-frame, 2 minutes?

Best Practices: Design

- Force communication through firewall system
  - Between the wired and wireless infrastructure
- Deploy IDS solution
- Disable file sharing between wireless clients
- Evaluate use of static IP addressing and disabling of DHCPs for mobile devices
- At least 128-bits or as large as possible

Defense-in-Depth



Best Practices: Access Points

- Minimize number of access points
- Implement strong physical access controls
- Install access points away from exterior walls
- Change the default SSID
- Evaluate disabling the broadcast SSID feature so that the client SSID must match that of the AP
- Disable all unnecessary protocols
- Ensure strong authentication for all APs
- Review logging capabilities of APs
  - Review log files regularly

Best Practices: Mobile Devices

- Install personal firewall software on all wireless clients
- Install anti-virus on all wireless clients Label all handheld devices with owner and organization information
- Inform all employees where to report a lost or stolen device
- Enable a “power-on” password for all devices
  - Recommend strong passwords for access
- Implement auto-logoff capabilities

Thank You!

- Email your testimonial and receive a free HIPAA Security quick reference card
  - Pabrai@HIPAA**Academy**.Net
- Check out the e-store at:
  - www.HIPAA**Academy**.Net

HIPAA ACADEMY™
HIPAAacademy.Net