# Health care & HIPAA

# Security Remediation

eHIPAA ACADEMY™
HIPAAacademy.Net

Uday O. **Ali** Pabrai, CISSP, CHSS
Chief executive, HIPAA Academy

# Security Challenges

- Password management
- Malicious software
- Wireless proliferation
- Contingency planning
- Auditing

# Remediate

- **Launch Activities**
  - Deploy Firewall Solutions, IDS/IPS
  - Secure Facilities & Server Systems
  - Deploy Device & Media Control Solutions
  - Implement Identity Management Solutions
  - Deploy Access Control Solutions
  - Implement Auto-logoff Capabilities
  - Deploy Integrity Control and Encryption
  - Develop & Test Contingency Plans
  - Activate Auditing Capabilities

eHIPAA ACADEMY™
HIPAAacademy.Net

# Wireless Security: Getting Started

- **Conduct risk analysis**
- **Develop security policies**
  - **Establish best practices**
    - Design
    - Access points
    - Mobile devices
- **Remediation: Design infrastructure**
  - Firewall
  - IDS
  - Wired network

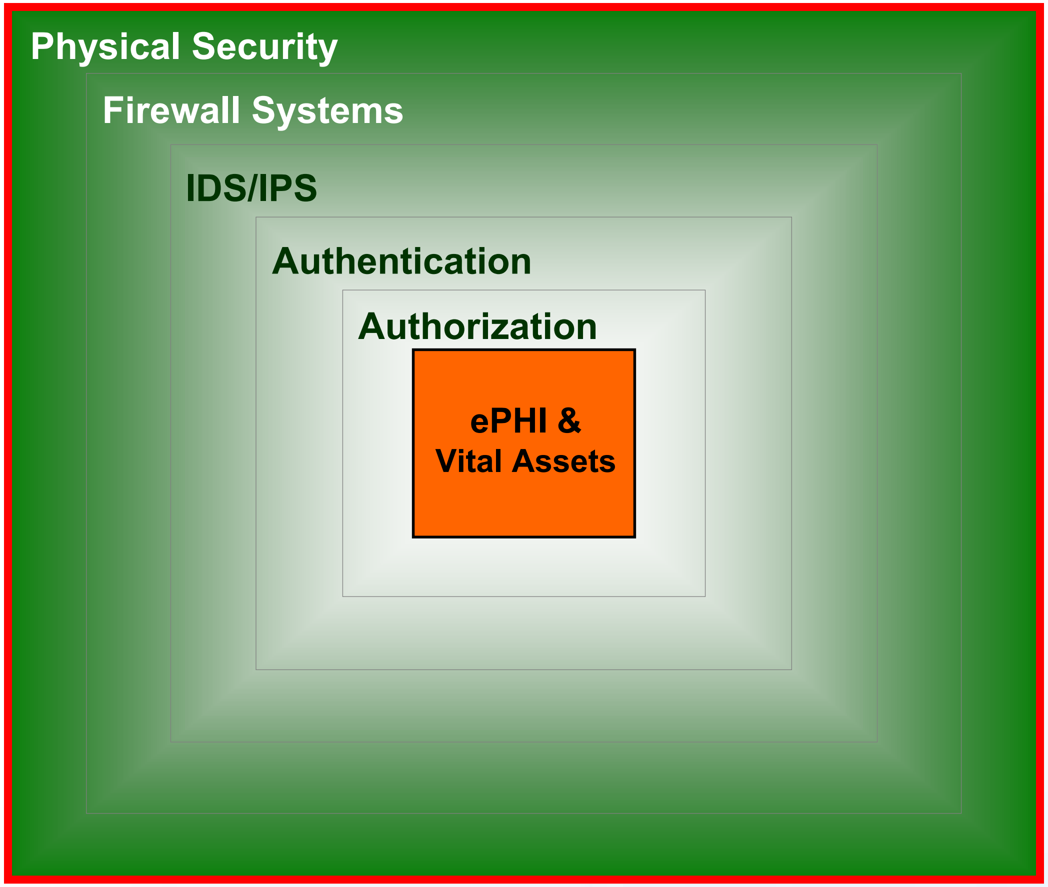
# Best Practices: Design

- 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

# 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

# Summary: Defense-in-Depth



Physical Security

Firewall Systems

IDS/IPS

Authentication

Authorization

ePHI & Vital Assets

# Thank You!

- Uday Ali Pabrai
  - Pabrai@HIPAA**academy**.Net