Risk Analysis and HIPAA Security

Uday O. Ali Pabrai, CHSS, SCNA

Chief Executive and Co-Founder, HIPAA Academy

Objective

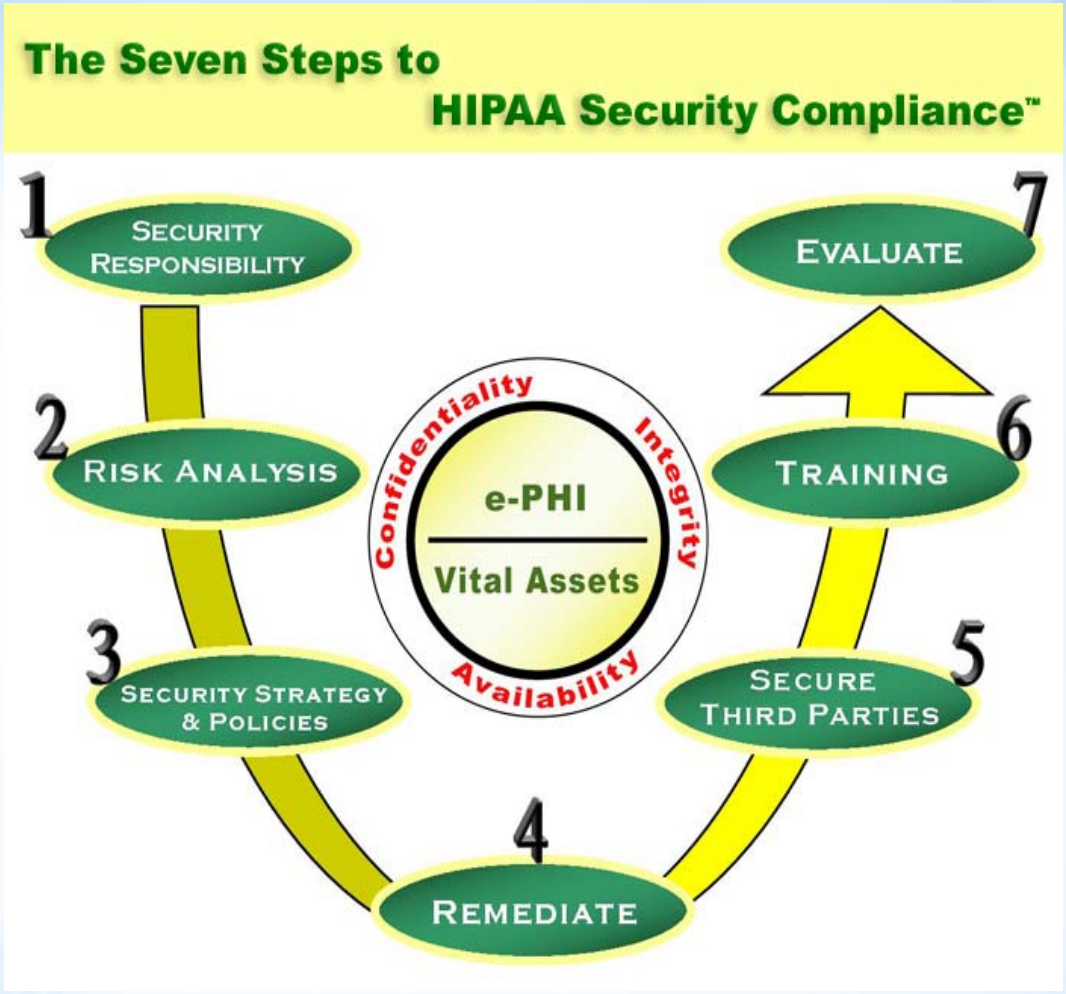
- Definition
- Seven Steps to HIPAA Security
- Step 2: Risk Analysis
  - Scope
  - Phases
  - Getting Started
- Bottom line

Definition

- Process to identify relevant assets and threats
- Identifies potential safeguards to mitigate critical risk
- A HIPAA Security Rule requirement

- **Establish the “State of Risk” associated with the Organization**

Seven Steps to HIPAA Security



Scope

- Risk Analysis is Step 2
- It includes addressing the areas of:
  - **Vulnerability Assessment**
    - **Scanning Tools**
  - **Business Impact Analysis (BIA)**
    - **Critical Business Functions**
  - **Information System Activity Review**
    - **Audit Logs**

Phases of Risk Analysis

- Phase I: e-PHI Documentation
  - **Document e-PHI Flow, Vital Systems**
- Phase II: e-PHI Risk Assessment
  - **Identify Vulnerabilities**
  - **Recommend Safeguards**
- Phase III: e-PHI Safeguards Determination
  - **Likelihood of Risk**
  - **Impact to e-PHI**
  - **Remaining Risk to e-PHI**

Getting Started

- Phase I: e-PHI Documentation
  - e-PHI Flow Diagrams
  - Network Diagrams
  - Asset Inventory
  - Risk Assessment Surveys
- Phase II: e-PHI Risk Assessment
  - HIPAAShield™ BIA Report
  - HIPAAShield™ Vulnerability Report
- Phase III: e-PHI Safeguards Determination
  - **HIPAAShield™ Risk Analysis Report**

Bottom line

“We must be compulsive about managing risk.”

PDF on “HIPAA Security and Risk Analysis” Available at:

HIPAA**Academy.**Net