Applying Technical Solutions

The ables

- Addressable
- Arguable
- Reasonable

§164.306 General Rules

- §164.306(a) Covered entities must do the following:
  - §164.306(a)(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
  - §164.306(a)(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
  - §164.306(a)(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required.
  - §164.306(a)(4) Ensure compliance by its workforce.

§164.306(b) Flexibility of Approach

- §164.306(b)(1) Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.
- §164.306(b)(2) In deciding which security measures to use, a covered entity must take into account the following factors:
  - §164.306(b)(2)(i) The size, complexity, and capabilities of the covered entity.
  - §164.306(b)(2)(ii) The covered entity's technical infrastructure, hardware, and software security capabilities.
  - §164.306(b)(2)(iii) The costs of security measures.
  - §164.306(b)(2)(iv) The probability and criticality of potential risks to electronic protected health information.

Implementation Specifications

- §164.306(d) Implementation specifications.
  - §164.306(d) (1) Implementation specifications are required or addressable. If an implementation specification is required, the word "Required" appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word "Addressable" appears in parentheses after the title of the implementation specification.
  - §164.306(d)(2) When a standard adopted includes required implementation specifications, a covered entity must implement the implementation specifications.
  - §164.306(d)(3) When a standard adopted includes addressable implementation specifications, a covered entity must—

Addressable Standards

- §164.306(d)(3)(i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic protected health information; and
- §164.306(d)(3)(ii) As applicable—
  - §164.306(d)(3)(ii)(A) Implement the implementation specification if reasonable and appropriate; or
  - §164.306(d)(3)(ii)(B) If implementing the implementation specification is not reasonable and appropriate—
    - §164.306(d)(3)(ii)(B)*(1)* Document why it would not be reasonable and appropriate to implement the implementation specification; and
    - §164.306(d)(3)(ii)(B)*(2)* Implement an equivalent alternative measure if reasonable and appropriate.

Risk Analysis 164.308.a.1 (R)

- Network Based Scanners TCP/IP
  - Simulate behavior of attackers to expose vulnerability
  - Have policy based configuration - COTS
  - Have configuration file - Free
  - Configuration file or policy launches multiple programs
  - Must be run from a multi threaded operating system
  - Exploits designed to expose vulnerabilities
  - Additional exploiting required

Risk Analysis 164.308.a.1 (R)

- Network Based Scanners
- All have strengths and weaknesses
  - Internet Scanner
  - Security Analyzer
  - By-Control
  - NMAP
  - Sara
  - Satan
  - Nessus

Risk Analysis 164.308.a.1 (R)

- Host Based Scanners
  - Check for consistencies in the corporate security policy
  - Enforce security policy
  - Installed on the Host Machine
  - Detects vulnerabilities
  - Can be multi platform

Risk Analysis 164.308.a.1 (R)

- Host Based Scanners
  - System Scanner- Internet Security Systems
  - Security Analyzer – NetIQ
  - By-Control - Bindview Corp
  - ECM – Configuresoft

Information System Activity Review 164.308.a.1 (R)

- Host Based Intrusion Detection
  - Monitors a systems applications log files
  - Responds with an alarm
  - Responds with countermeasure

Information System Activity Review 164.308.a.1 (R)

- Host Based Intrusion Detection
  - Mantrap- Recourse Technologies
  - Netvision Policy Management- NetVision
  - Tripwire for Servers- Tripwire Inc
  - Enterprise Security Solution - Bindview

Isolate Clearinghouse function 164.308.a.4 (R)

- Network Architecture
  - VLANS – switching and routing traffic
  - Servers – were they reside
  - Email – content security and encryption
  - Firewall– control communications

Isolate Clearinghouse function 164.308.a.4 (R)

- Firewall
    - System or group of systems that enforces an access control policy between networks
- Firewall Technology
    - Cisco PIX
    - Checkpoint Firewall 1
    - Storm Watch

Protection from Malicious Software 164.308.a.5 (A)

- Denial of Service (DOS attack)
  - Smurf attack
  - Buffer Overflow attack
  - Syn attack
  - Teardrop attack

Protection from Malicious Software 164.308.a.5 (A)

- Denial of Service (DOS attack)
  - Smurf attack
  - Buffer Overflow attack
  - Syn attack
  - Teardrop attack

Protection from Malicious Software 164.308.a.5 (A)

- Worms
- Viruses
- Protection
  - Server based
  - Workstation based

Protection from Malicious Software 164.308.a.5 (A)

- Denial of Service (DOS attack)
  - Smurf attack
  - Buffer Overflow attack
  - Syn attack
  - Teardrop attack

Protection from Malicious Software 164.308.a.5 (A)

- Anti Denial of Service (DOS attack) tools
  - Attack Mitigator – Top Layer Networks
  - Pest Patrol – Pest Patrol Inc.
  - ManHunt – Recourse Technologies
  - NetDirector – Niksum Inc

Contingency Plan 164.308.a.5 (A)

- Disaster Recovery Plan Software
  - Relational databases built on word processing capabilities to develop and maintain disaster recovery plans
  - Recovery – SunGuard
  - LDPRS – Strohl Systems

Device and Media Controls 164.310.d.1 (R)

- Disposal
  - Cyber scrub
- Re-image
  - Drive Copy
  - Drive Image

Workstation Security 164.310.c. (R)

- Harden
  - Policy for hardening all desktop configurations
  - Secure Operating System
  - Policy on workstation use
- Data at rest encryption (laptop)
  - Grim Card
  - Cyber Dog

Access Control 164.312.a (A)

- Encryption and Decryption
  - Sophisticated computer algorithms are use to encrypt the files in storage (at rest) then decrypt when needed,

Data at rest Servers and Applications

- Ancort
- Grimdisk
- Cryptodisk

Audit Controls 164.312.b (R)

- Real Time Security Awareness
  - See what is happening across the enterprise from a single console.
  - Back up log files from a single location
  - Cost justified by reduction in personnel
- RTSA
  - Manhunt
  - NetForensics
  - NSAG First Assurance

Integrity 164.312.c (A)

- Public Key Infrastructure (PKI)
  - Desktop - Email
  - Network - VPN
  - Cost justified by reduction in personnel
- Verify Designated Record Set (DRS) has not been modified.

Transmission Security 164.312.e (A)

- Integrity Controls
  - VPN
  - VLAN
  - Email Encryption
- Encryption
  - IPSec
  - PPTP
  - Router and VPN driven encryption schemas

HIPAA PROS.com

CHC Healthcare Solutions

Enterprise Solutions

- Enterprise Security Administration
  - NetVision Policy Management Suite
  - Real Secure Site Protector
  - By-Admin
- Key benefits:
  - Tool that provides enterprise wide security administration
  - Keeping track of user access and across the enterprise
  - Role based access built in to access control model