HIPAA Security:
The Essence of What Matters

HIPAA Summit 7
Baltimore, MD
14 September 2003

ses
Secure Enterprise Solutions

Thomas Welch

- CEO of Secure Enterprise Solutions Inc.
- Former Law Enforcement Officer (Broward County, FL)
- UNIX/C Developer – 10 Years
- Certified Information System Security Professional (CISSP)
- Certified Protection Professional (CPP)
- e-mail: twelch@sendsecure.com

Agenda

- What is HIPPA Security?
- What Matters?
- Information Security Lifecycle
- Cost of Not Planning
- Q&A

What is HIPAA Security?

Congressional Bafflegab

or

Prudent Regulation?

What is HIPAA Security?

- A literal interpretation would indicate an impossible task
  - Use of the word “ensure” is troubling at best
    - You can’t ensure security
    - You can only ensure the effort
- A “reasonableness” interpretation would indicate a prudent business practice
  - You already have a fiduciary responsibility to secure patient records
  - The responsibility is no different for any other industry

Understanding HIPPA Security

- It’s a complex problem involving:
  - People (Behavioral)
  - Technology
- Like all complex business processes, it must be broken down to manageable task
- Break down the regulation to the THINGS THAT MATTER!

What Matters?

- Leadership Matters
- Policies Matter
- Training Matters
- Risk Management Matters
- Technology Matters

Leadership Matters

- Identifies a single responsible individual and establishes accountability
  - Naming a Security Officer is the only effective way to build accountability into the process
- Security, like all other important business processes, must start at the executive level
  - Budgets
  - Resources
  - Direction

Policies Matter

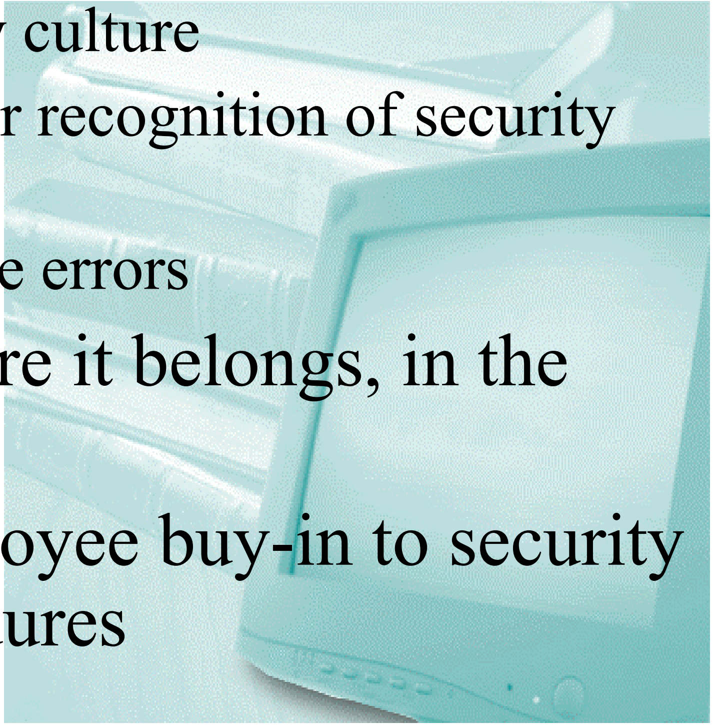
- Policies establish organizational directives
  - They provide essential guidance
  - They are the foundation of the information security program
  - They must be, both, enforceable and enforced
- Standards and Procedures must also be addressed
  - "Best Practice" Standards
  - Incident Response Planning
  - Business Continuity Planning

Security Policies

- **HR Policies**
  - Monitoring Awareness
  - Privacy Issues & 1st Amendment Rights
  - Company Equipment Use
  - Who Owns the Data
- **Operational Policies**
  - Internet & Intranet Usage
  - Passwords
  - E-mail usage
  - File transfers & Attachments
  - Virus Control
  - Data Classification Sensitivity
- **Moral & Ethical Conduct**
  - Etiquette and Proper Usage
  - Pornography
  - Harassment
- **Legal Responsibilities, Penalties & Enforcement**
  - Warning Notice
  - Incident Response Plan
- **Administrative Policies**
  - Sanctions
  - Workforce Clearance
  - Separation Policy
  - Media Reuse & Destruction

Training Matters

- Helps the entire staff better understand security issues, risks and threats
  - Creates a security culture
  - Allows for greater recognition of security events
  - Helps to minimize errors
- Puts security where it belongs, in the forefront
- Helps foster employee buy-in to security policy and procedures



Risk Management Matters

- You must understand the problem, before it can be resolved
- Risk Management Process
  - Risk Assessment
  - Risk Reduction
  - Risk Transfer
  - Risk Acceptance
- Risk Analysis Vital!

Risk Management Matters

- What could happen (threat event)?
- If it did happen, how bad could it be (threat impact)?
- How often could it happen (threat frequency)?
- How certain are the answer to the first three questions (recognition of uncertainty)?

Risk Management Matters

- What is the Risk that:
  - PHI will be used/disclosed inappropriately on:
    - Internet transmissions?
    - Wireless LANs?
    - Tele-worker Workstations?
    - Portable Devices (Hand-helds, PDAs)?
  - Passwords will be compromised?
  - Security incidents will go undetected?
  - "Social engineering" will result in unauthorized access?

Risk Management Matters

- Complete at least a ‘minimal’ Gap Analysis
  - Information Security Assessment
  - Vulnerability Testing
- Asset Identification and Classification
- Fix the easy stuff
- Do what’s practical and cost effective
- Document what you plan to do/not do, and why
- Finally, you need to be systematic about security

Risk Management Matters

- Administrative Safeguards
  - 12 Required
  - 11 Addressable
- Physical Safeguards
  - 4 Required
  - 6 Addressable
- Technical Safeguards
  - 4 Required
  - 5 Addressable

Note: The concept of “addressable implementation specifications” was introduced to provide covered entities with additional flexibility with respect to compliance with the security standard.

Technology Matters

- Design a Secure Architecture
- Services for a Trusted Environment
  - Confidentiality
  - Integrity
  - Availability
  - Identification & Authentication
  - Authorization & Access Control
  - Non-repudiation

ses
Secure Enterprise Solutions

Technology Matters

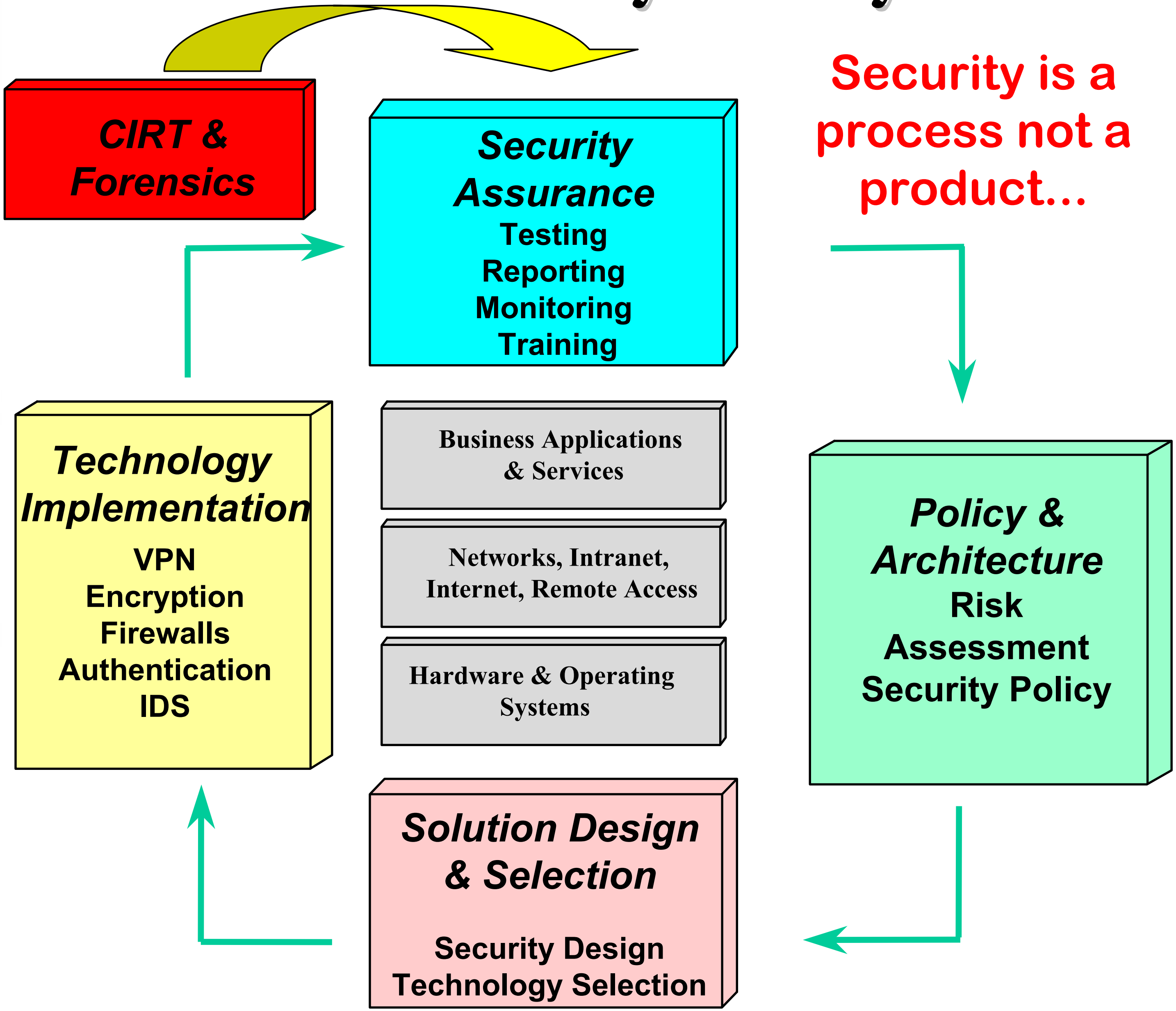
- Select & Implement Countermeasures
  - Firewalls
  - IDS
  - Standardized hardware-software platforms
  - Host Hardening
  - Strong Authentication & Access Control (w/Auditing)
  - Integrity Controls (i.e. Tripwire)
  - Encryption and VPNs
  - Virus protection

10101010101010 ses
Secure Enterprise Solutions

Information Security Lifecycle

Building Blocks

- People
- Process
- Technology



Security is a process not a product...

CIRT & Forensics

Security Assurance
Testing
Reporting
Monitoring
Training

Policy & Architecture
Risk
Assessment
Security Policy

Solution Design & Selection

Security Design
Technology Selection

Technology Implementation
VPN
Encryption
Firewalls
Authentication
IDS

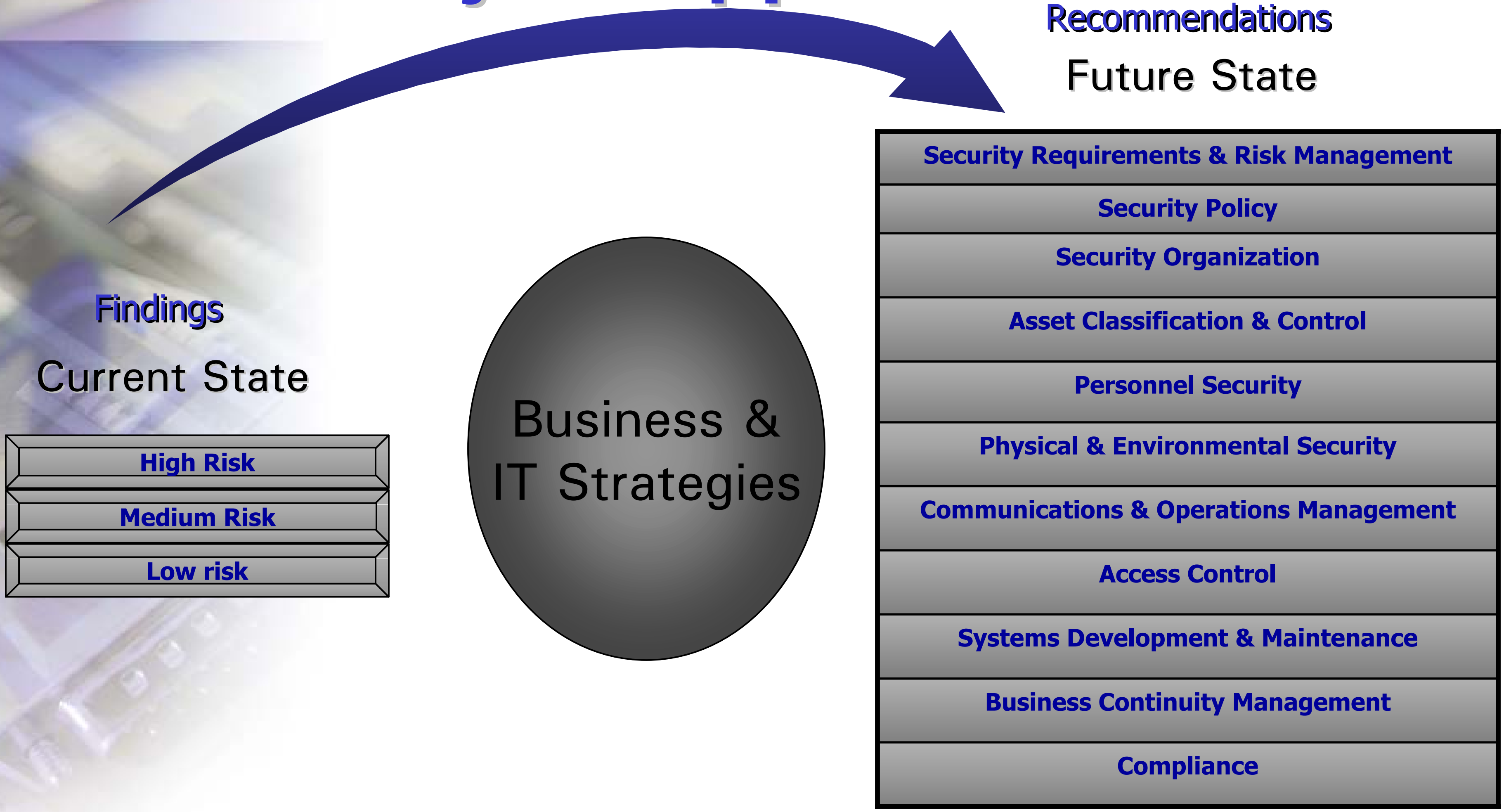
Business Applications & Services

Networks, Intranet, Internet, Remote Access

Hardware & Operating Systems

ses
Secure Enterprise Solutions

Project Approach



Recommendations

Future State

Security Requirements & Risk Management

Security Policy

Security Organization

Asset Classification & Control

Personnel Security

Physical & Environmental Security

Communications & Operations Management

Access Control

Systems Development & Maintenance

Business Continuity Management

Compliance

Business & IT Strategies

Findings

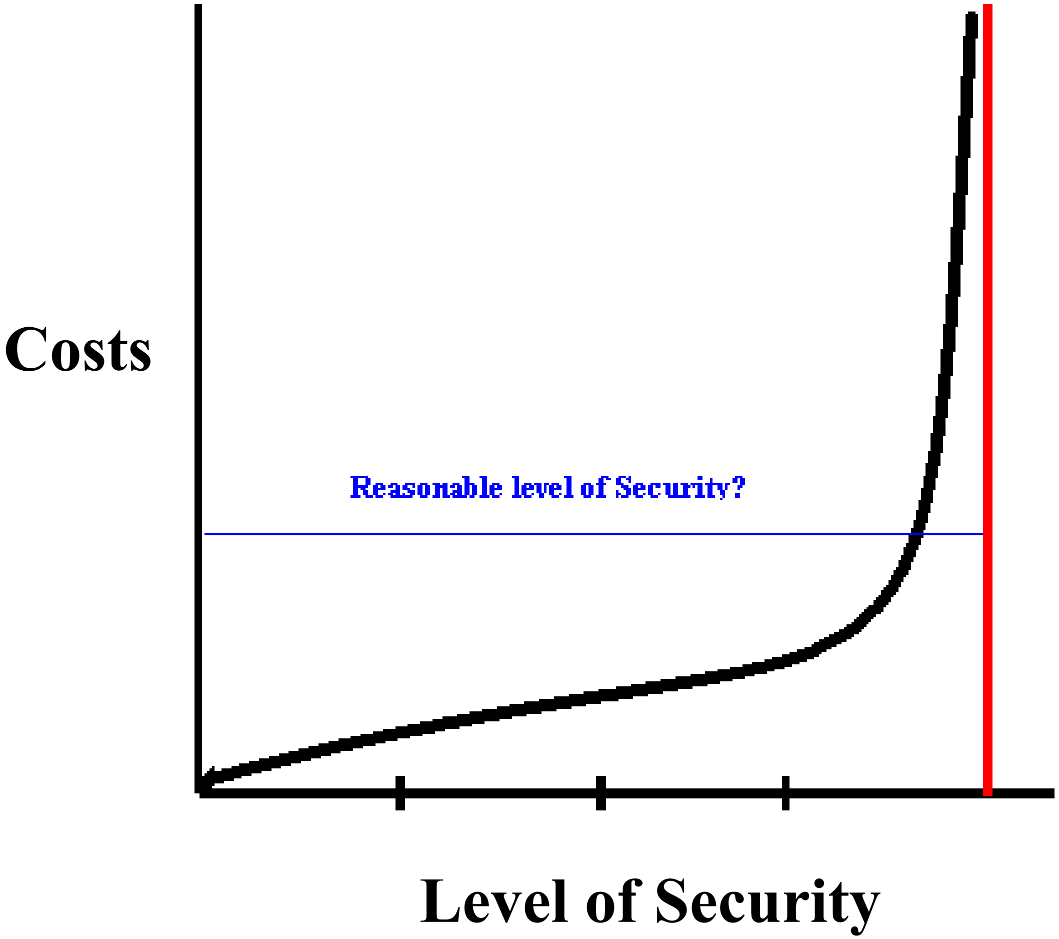
Current State

High Risk

Medium Risk

Low risk

The Cost of Security



Secure Enterprise Solutions

Risk Management Model

FEAR

TRUST

The level of impact to each critical asset is estimated based on the relationship between the threat and vulnerability.

Threats to Your Organization

- “Acts of God”
- People (Hackers, Crackers, O.C., etc.)
  - Error and Omissions
  - Remote Employees
  - Malicious and Criminal Behavior
- Insecure Applications
- Information Warfare/ Cyber Threat
- Loss of Data from Malicious Code and Viruses
- Civil Liability

ses
Secure Enterprise Solutions

No one is immune!

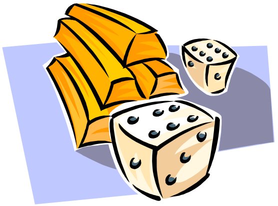
…and the threat is increasing.

Why is the Threat Increasing?

- Increased Computer Use
- More Technical Population
- Global Networks and Broadband Technologies
- Insecure Systems*
- Dependency on Computers
- No Real Deterrents
- Lack of Ethics
- Many “Good” Tools
- Increased Anonymity

Cost of Not Planning Security

- Financial Loss
  - Lost Revenue, Loss of Trade Secrets or IP, Embezzlement, Extortion, etc.
- Loss of Customer Confidence
- Embarrassment
- Increased Liability
  - Failure to follow a “Standard of Due Care”
  - Failure to Protect “Private” Data
  - Third-party Liability



Information Security

- Security is more than just a Login
  - It MUST be implemented in layers
- Security should be as transparent as possible
- An organization must be ready to protect, detect, and respond to any type of adverse event.

Questions & Answers

Administrative Safeguards

Standards	Sections	Implementation Specification	R/A	T
Security Management Process	164.308(a)(1)	Risk Analysis	R	
		Risk Management	R	
		Sanction Policy	R	
		IS Activity Review	R	
Assigned Security Responsibility	164.308(a)(2)		R	
Workforce Security	164.308(a)(3)	Authorization and/or Supervision	A	
		Workforce Clearance Procedures	A	
		Termination Procedures	A	
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function	R	
		Access Authorization	A	**Y**
		Access Establishment and Modification	A	**Y**
Security Awareness and Training	164.308(a)(5)	Security Reminders	A	
		Protection from Malicious Software	A	**Y**
		Log-in Monitoring	A	**Y**
		Password Management	A	
Security Incident Procedures	164.308(a)(6)	Response and Reporting	R	**Y**
Contingency Plan	164.308(a)(7)	Data Backup Plan	R	**Y**
		Disaster Recovery Plan	R	**Y**
		Emergency Mode Operation Plan	R	**Y**
		Testing and Revision Procedure	A	
		Applications and Data Criticality Analysis	A	
Evaluation	164.308(a)(8)		R	
BA Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement	R	

Physical Safeguards

Standards	Sections	Implementation Specifications	R/A	T
Facility Access Controls	164.301(a)(1)	Contingency Operations	A	
		Facility Security Plan	A	
		Access Control and Validation Procedures	A	Y
		Maintenance Records	A	
Workstation Use	164.310(b)	Documented procedures for system use	R	Y
Workstation Security	164.310(c)	Physical placement and control	R	Y
Device and Media Controls	164.310(d)(1)	Disposal	R	Y
		Media Re-use	R	Y
		Accountability	A	
		Data Backup and Storage	A	Y

Technical Safeguards

Standards	Sections	Implementation Specifications	R/A	T
Access Controls	164.312(a)(1)	Unique User Identification	R	**Y**
		Emergency Access Procedure	R	**Y**
		Automatic Logoff	A	**Y**
		Encryption and Decryption	A	**Y**
Audit Controls	164.312(b)		R	**Y**
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic PHI	A	**Y**
Person or Entity Authentication	164.312(d)		R	**Y**
Transmission Security	164.312(e)(1)	Integrity Controls	A	**Y**
		Encryption	A	**Y**

Planning for the Worst Case

- Loss of Intellectual Property
  - Theft
  - Data Loss or Destruction
- Hack Attack
  - Breach of Confidentiality
  - Loss of Data Integrity (Data Manipulation)
- Virus Contamination and Worms
  - Organizational Impact of Nimda and Code Red
- Distributed Denial of Service (DDoS) Attack
  - It Can Happen to Yahoo, eBay and others
  - Loss of System Availability
- Cyber Terrorism