



HIPAA Compliance for Mobile Healthcare

Peter J. Haigh, FHIMSS

Verizon

peter.haigh@verizon.com



Workgroup for
Electronic Data Interchange

Comply or ...

**MARTHA
STEWART**

Living
BEHIND BARS

jailhouse chili
cooking for a crowd

faux finishes
brighten up drab
cell blocks with color

cozy cots
decorating sheets

prison parties
sprucing up your cell
for those special
holiday occasions

good things
polishing handcuffs
and leg irons

laundry room
removing pesty blood
stains from prison garb

cellkeeping

VOLUME 1 • NUMBER 1
published 10 times a year for the next 30 years
www.marthastewart.com



Context - Privacy & Security under HIPAA

- ◆ Privacy is what you have already promised to do, since 4/14/2003
- ◆ Security is about how you fulfil that promise now as well as in 4/2005 (“stop-gap” security)
- ◆ Networks are how the authorized (and unauthorized) get PHI
- ◆ Improper network activity specifically identified as a “Security incident”
- ◆ Wireless networks have special vulnerabilities
- ◆ Remote network nodes have access risks
- ◆ **Therefore network security is of paramount importance**



Securing the Network

◆ Sources of Security Threats

- Insiders/outside = 70/30, maybe 80/20
 - Malicious, dishonest, corrupt, distracted, disgruntled, negligent
 - Naturally curious, poorly trained, terminated
- Terrorists
- Hackers & Crackers
- Computer criminals

◆ Securing the Network Perimeter

- Outsiders & remote users

◆ Policy, Training, Access Control, Monitoring, etc.

- Insiders

◆ Beware of outdated or “crustacean” security

Other Security Issues

◆ What is being transmitted?

- Video, audio
- Test results
- Medical Records & Images
- Medical intervention

◆ Quality & reliability

- Is network outage “life-threatening”?
- How good does resolution have to be?
- How long does it take to download the images, etc?

A photograph of a large, multi-towered stone castle, likely a Norman or Celtic tower house, with a wooden walkway leading to the entrance. The castle is situated on a grassy bank next to a body of water. The sky is a clear, bright blue. The text is overlaid in the center of the image.

**State of the Art
Security
pre-Gunpowder!**



Today's main topics

- ◆ **A HIPAA Security primer**
- ◆ **Technical Solutions for Security Compliance**
- ◆ **Wireless Technology Overview**
- ◆ **What to do!**



What changed in the Final Security Regulations?

- ◆ **Alignment with the Privacy Regulations**
- ◆ **Services & mechanisms = Technical Safeguards**
- ◆ **69 required implementation specifications (RIS) reduced to 13 (20 including subsections)**
- ◆ **22 addressable implementation specifications (AIS)**
- ◆ **New Definition of Electronic Media**
 - Voice (including voice-mail and video teleconferencing) & “paper to paper” fax not covered
 - Voice response & “faxback” are covered
 - What about Voice & Video over IP?
- ◆ **More regulations to come**
 - Electronic signature
 - Non-electronic PHI
 - Enforcement
- ◆ **But, no “evolving versions”**



What's the Risk??

- ◆ **Risk Analysis is MANDATORY!**
- ◆ **What is the Risk that... (just a few examples):**
 - **PHI can be used/disclosed inappropriately on:**
 - Internet transmissions?
 - Wireless LANs?
 - Tele-worker Workstations?
 - Portable Devices (Hand-helds, PDAs)?
 - **Passwords can be compromised?**
 - **Security incidents go undetected?**
 - **“Social engineering” will result in unauthorized access?**
- ◆ **Document what you plan to do/not do, and why!**



Security Standards Matrix

◆ Administrative Safeguards

- 11 Addressable
- 12 Required

◆ 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.



HIPAA v. ISO Standards

◆ Administrative Safeguards

- Organizational Security
- Information Security Policy
- Personnel Security
- Business Continuity Management
- Compliance

◆ Physical Safeguards

- Physical & Environmental Security

◆ Technical Safeguards

- Asset Classification and Control
- Access Control
- Communications and Operations Management
- Systems Development and Maintenance



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



Steps to Technical Compliance

- ◆ **Conduct a Thorough Risk Assessment**
- ◆ **Evaluate the Risks**
- ◆ **Design a Secure Architecture**
- ◆ **Select & Implement Countermeasures**
 - Firewalls
 - IDS/IPS
 - Standardized hardware-software platforms
 - Host Hardening
 - Strong Authentication & Access Control (w/Auditing)
 - Integrity Controls (i.e. Tripwire)
 - Encryption and VPNs
 - Virus protection
- ◆ **Conduct Follow-up Audits (Quarterly)**
- ◆ **Establish Evidence that You're "Doing Something"**
 - **Waiting is Risky Business**





Why Remote & Mobile?

◆ Cost & convenience

- Telecommuting
- Access from another workplace
- Access to specialized services

◆ The special value of mobility

- Anywhere, anytime access to medical data & messages
- Effectiveness & efficiency improvement for MDs
- Faster intervention for patients

◆ Patient convenience

- Travel avoidance
- Access to “unreachable” resources
- Remote monitoring of chronic conditions/diseases



Mobile Technology Alternatives

◆ DSL/Cable

- Low cost “broadband”
- Speeds from 1.5Mb/128Kb to 7.1Mb/768Kb
- “Always on” convenience

◆ WiFi (IEEE 802.11a/b/g)

- Easy to install
- Cost falling rapidly
- Public “hot-spots” increasingly available

◆ Cellular Data

- True freedom to connect from (almost) anywhere

◆ Satellite

◆ Dial-up Internet access

- Least desirable/reliable
- BUT inexpensive and ubiquitous



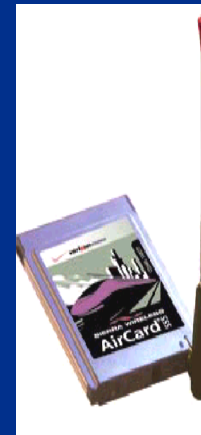
Cellular Data Service Highlights

◆ Express Network

- “Always-On” internet connection
- Average speeds 40 to 60 kbps
 - Burstable to 144 kbps
 - Higher effective rates with Venturi compression software
- VPN Client enables access:
 - Email
 - Corporate applications
- Sierra Wireless AirCard 555 (internal model)
- Mobile Office kit for EN enabled phones

◆ Faster access coming

- EVDO=1.2-2Mbps
- Already in San Diego and DC, 10 more areas in 2004, nationwide in 2005



+





Remote & Mobile Security Issues

- ◆ **“Always on” vulnerability**
 - **Hacking exposure**
 - To the remote PC
 - To the corporate network
 - **Zombies for DDOS attacks**
 - **Wireless = Broadcast**
- ◆ **“War driving”**
- ◆ **Rogue access points**
- ◆ **Unknown/bogus sign-ons**
- ◆ **Insecure surroundings (patient/teleworker homes)**
- ◆ **Proprietary vs. Standard security provisions**



Security Tools for HIPAA Compliance

- ◆ **Firewalls**
 - “Personal” Firewall
 - “True” Firewall (managed?)
- ◆ **IDS/IPS**
- ◆ **Secure switches**
- ◆ **Anti-virus**
- ◆ **Two-factor authentication**
- ◆ **Secure VPN**
 - IPSec
 - SSL
 - Digital certificates
- ◆ **IEEE 802.11i/Robust Security Network (RSN) is coming**



Technical Compliance Summary

- ◆ **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
 - Respond... to any type of adverse event
- ◆ **The **GOOD NEWS** – many tech available to improve security**

