









HIPAA Strategies

Gary Christoph, Ph.D. Sr. VP Government and Healthcare gchristoph@seclarity.com 410-884-1313

April 8, 2005

A Blumberg Capital, Valley Ventures and Intel Capital Funded Security Company

Seclarity, Inc. 11705 Lightfall Court Columbia, MD 21044



The Issue

- Recent Compliance Mandates (HIPAA, GLBA, SarbOx, etc.) are (unfortunately) strong security drivers
- Network Security is Hard and Expensive
- Use a "Common Sense" approach



HIPAA

Title II Administrative Simplification

Transaction Standards

Security

Standard Code Sets

Unique Health Identifiers

Privacy

Administrative Procedures

- Chain of Trust Agreement
- Certification,
- Internal Audit, Training, Written Policies & Procedures, etc.

Physical Safeguards

- Secure Workstation
- Physical Access Controls, Media Controls, etc.
- Security Awareness
- Training

Technical Security Services

- Access Controls
- Authorization
- Data Authentication
- Entity Authentication

Technical Security Mechanisms

- Basic Network Safeguards
- Integrity and Protection

Limitations

• Covers Protected Health Information (PHI) transmitted or stored, in any medium (electronic, paper, oral)

General Rules

- · PHI data elements defined
- Notice of Privacy Practices mandated
- Minimum necessary disclosure/use of data
- Consent required for routine use
- Authorization required for non-routine use
- Business associate contracts required
- Designated Privacy Officer

Electronic Signature

Not currently required



What Does HIPAA Really Require?

YOU MUST:

- Think about the risks you face
- Develop coherent, enforceable policy
- Write it down
- Implement/operate whatever controls this requires
- Train/educate staff
- Periodically test & document



Compliance Issues:

- Policy is not written down
- Written policy is not followed
- Implementations are not "fire and forget"
- Consultants aim to make money, not fix the problem



Hard NW Security/Privacy Issues:

- People are involved
 - People are neither repeatable nor logical
 - People on the job make inappropriate assumptions
- Technical Solutions are too complex
 - Point products do not tile the floor
 - Management of many solutions is not easy or cheap
 - Pace of technological change adds new vulnerabilities (e.g., wireless)
- Administrative Solutions that are not
 - Processes get in the way of work
 - Controls violated without your knowledge or without consequence



A Simple Strategy:

- Decide what is important to protect
- Find a simple way to protect it
- Document it



The Regs were written to be scalable and technology neutral. Why?

- Rules have to cover everything from a oneperson Dentist's office in Podunk, Missouri, to Johns Hopkins Hospital
- It economically makes no sense to require everyone to have the same controls
- Technology evolves

Therefore:

The solution must fit the need

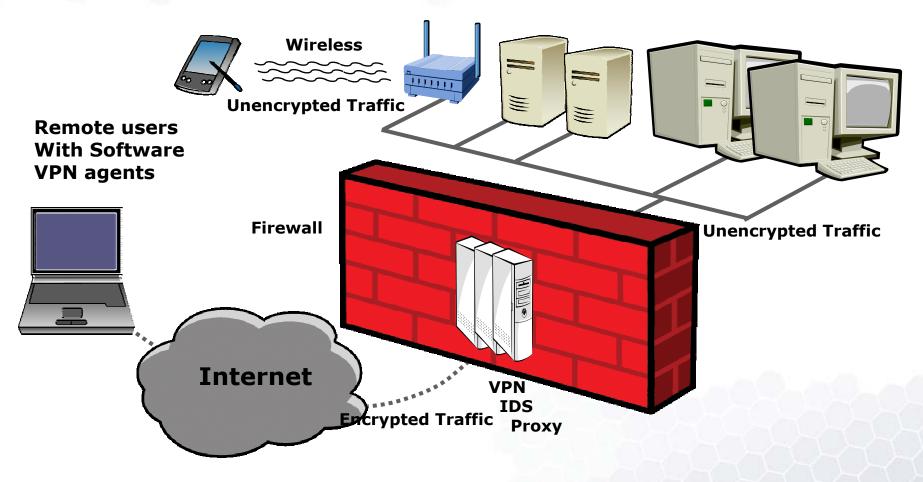


Technical Solution Target

- Want transparency
 - Easy for users to comply
 - Easy for admins to enforce
- Want universality
 - Everywhere same policy enforced the same
 - Use technology to reduce administrative controls
- Want simplicity
 - Complexity is the enemy
 - Easy to manage
- Want verifiability
 - Documentable
- Want cheap
 - Do not want to go out of business



A Simplified View of a Contemporary "Secured" Network:





A Simple view of an Endpoint-Secured Network:

