1.02 Last Minute Security Compliance - Tips for Those Just Starting

10th National HIPAA Summit

April 7, 2005

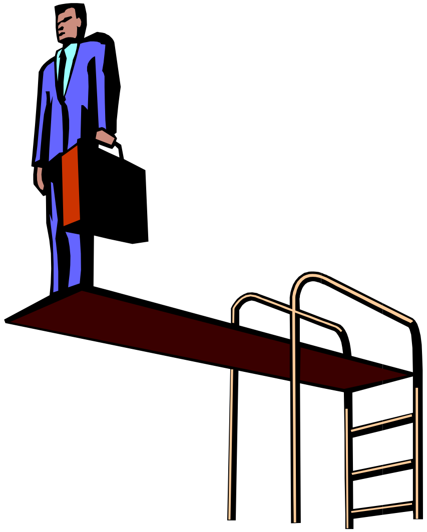
Chris Apgar, CISSP – President
Apgar & Associates, LLC, former HIPAA Compliance Officer for Providence Health Plans

Presentation Overview

- What are the worries
- Internal & External Risks
- Steps to address risks
- What is a firewall and why is it needed
- Malicious code or viruses
- Transmitting information securely
- Resources
- Summary

What are the Worries

- Wireless security
- Portable devices
- Encryption/secure messaging
- Access control (including remote access)
- Employees and hackers



What are the Worries

- Employee termination
- Risk assessment
- Policies and procedures
- Social engineering
- Controlling access to your facility

What are the Worries

- Media disposal and re-use
- Staff training
- Anti-virus/spyware
- Password management
- Disaster planning

Steps to Take

- Risk assessment essential
- Risk management needed follow up
- Senior management buy in – risk avoidance isn’t always free
- Monitoring and auditing
- Utilize appropriate technology

Steps to Take

- Regulatory watch
- Open the closet – avoid hiding security and privacy incidents
- Stay current
- Take advantage of industry partnerships
- Consistency

Steps to Take

- The need to protect facilities and equipment
- Data center – critical to your business
- Changing locks and key cards
- Temporaries, contractors & volunteers
- Social engineering

Steps to Take

- Workstation security
- Secure storage (i.e., file cabinets, medical record shelving, etc.)
- Portable devices & dangers of theft and loss
- Remote access or teleworking
- Physical transport of PHI (media & hardware)

Steps to Take

- Policies and procedures
- Access control & Role-based access
- Password management
- Encryption or secure messaging
- Malicious code
- Spam

Steps to Take

- Internet use and misuse
- Intrusion detection
- Vulnerability detection
- Audit logs
- Backup & recovery
- Disaster & recovery/business continuation plan

Steps to Take

- Operating system security
- Laptop/PDA encryption
- Termination procedures
- Disposal of hardware and data
- Fitting technical security measures to need

Steps to Take

- Appointment of a security officer
- Staff training needs
- Cultural change
- Sanctions & enforcement
- Managing your workforce

Steps to Take

- Defining roles and “need to know”
- Minimum necessary applies
- Auditing requirements
- Record retention & retrieval
- Confidential faxing and other forms of sensitive communication

Firewalls & Why Use Them

- Allows wanted electronic traffic in and out of your organization
- Blocks damaging electronic traffic
- Firewall logs and what they mean
- Security against hackers

Firewalls & Why Use Them

- Hardware versus software firewalls – what's the difference?
- Available even to smallest organizations
- Hackers look for openings
- Protect your health information
- Acts as security guard

Malicious Software

- Viruses, trojans and worms
- Spyware
- Malicious cookies
- Spam
- E-mail threats

Malicious Software

- Anti-virus software and its use
- Anti-spyware and its use
- Anti-spam software and its use
- Built for small to large organizations
- The layered approach

Transmission Security

- "Clear text" versus encryption
- What is encryption?
- Compressed files not encryption
- File transfer protocol
- Virtual private networks

Transmission Security

- Web messaging
- Public key infrastructure
- Secure web sites
- Why encrypt?
- Inexpensive solutions

Resources

- Center for Medicare & Medicaid Services HIPAA Web Site: http://www.cms.hhs.gov/hipaa/hipaa2/default.asp
- National Institute of Standards & Technology (NIST): http://www.nist.gov
- Workgroup for Electronic Data Interchange: http://www.wedi.org

Resources

- HIPAA Assessment: http://www.nchica.org/activities/EarlyView/nchicahipaa_earlyview_tool.htm
- SANS: http://www.sans.org
- $(ISC)^2$: http://isc2.org
- HIMSS: http://himss.org

Resources

- The First Steps Toward Security: http://www.bindview.com/Resources/Articles/HealthData%20Mgmnt6-26.pdf
- RSA: http://www.RSA.com
- Tunitas Group: http://www.tunitas.com/
- National Institute of Health (regulatory information): http://list.nih.gov

Summary

- Nothing is risk free
- Remember to pay attention to internal and external threats
- Simple solutions equal quick compliance and sound business practice
- Firewalls are mandatory
- Malicious code or software can shut down your business
- Secure transmission of health information – accessible and necessary

Question & Answer

Chris Apgar, CISSP
President
Apgar & Associates, LLC
10730 SW 62nd Place
Portland, OR 97219
(503) 977-9432 (voice)
(503) 245-2626 (fax)
(503) 816-8555 (mobile)
Capgar@easystreet.com