15th National HIPAA Summit

Coordinating & Balancing Privacy, Security & Practical Operations

Chris Apgar, CISSP
President, Apgar & Associates, LLC
December 12, 2007

Overview

- Balancing business & security
- Security & privacy not all technology
- Placement of privacy & security – Organizational oversight
- Importance of risk analysis
- Other non-technical requirements
- Selling security
- Q&A

Balancing Business & Security

- DoD protection not required
- Risks are unavoidable
- Remember profitability
- Privacy & security solutions need to represent sound practice for the industry & the size & complexity of the organization

Balancing Business & Security

- HIPAA security rule flexible – take advantage of flexibility
- Expensive tools not always best protection
- Business needs to adopt security culture
- Users need to be involved – greatest risk area

Security & Privacy not all Technology

- HIPAA security rule – more than 1/3 administrative security
- Technology section not predominant section – support to administrative security
- Physical security may involve technology but often involves old fashioned keys & fire extinguishers

Security & Privacy not all Technology

- Privacy requires appropriate security but not necessarily technically specific solutions
- Privacy (and security) more people focused
- Technology important but needs to support needs of the business and sound administrative/physicial security requirements

Security & Privacy not all Technology

- Examples:
  - Access control administrative safeguard
  - Audit administrative & technical safeguard
  - Risk analysis administrative safeguard
  - Disaster recovery/emergency mode operations plans
  - Training
  - Policies & procedures

Security & Privacy not all Technology

- Examples (continued):
  - Patient privacy rights – primarily paper interface
  - Privacy covers non-electronic & many providers continue to rely on paper charts (even after EHR implementation)
  - Appropriate application security (e.g., EHR, bio-medical devices, PHR, etc.) lacking in today's applications
  - Secure e-mail relies on sender & recipient

Placement of Privacy & Security – Organizational Oversight

- Variations between organizations – who is appointed privacy and security officers (no matter the size)
- Generally security reports to IT
- Frequently privacy officer training lacking
- Frequently security officer non-technical training lacking

Placement of Privacy & Security – Organizational Oversight

- Authority & responsibility of privacy & security officers vary between organizations
  - Sometimes “only because HIPAA requires it”
  - Too often positions lack authority to force/effect change
  - Often responsibility exceeds authority
  - Important findings/risks overlooked

Placement of Privacy & Security – Organizational Oversight

- Privacy & security officers organizational placement vary
- Placement in organization needs to consider position effectiveness and perceived neutrality
- Positions need to be view as positions of trust

Placement of Privacy & Security – Organizational Oversight

- Appropriate placement of privacy officer in organization:
  - Compliance office
  - Legal
  - CEO/president
  - Senior executive with cross-organization responsibilities/authority

Placement of Privacy & Security – Organizational Oversight

- Appropriate placement of security officer in organization:
  - Compliance office
  - Legal
  - CEO/president
  - Senior executive with cross-organization responsibilities/authority
  - Not CIO

Placement of Privacy & Security – Organizational Oversight

- Positions need to be visible in positive way
- Heavy visible engagement in audits, risk analysis, policy/procedure development, etc.
- Interaction with local, state, federal standards development projects & bodies required

Importance of Risk Analysis

- HIPAA security rule requires risk analysis conducted regularly
- Foundation for security program:
  - Risk identification & mitigation
  - Policy & procedure development/ amendment
  - Disaster recovery/emergency mode operations plan building block
  - Audit criteria development
  - Workforce training content & requirements

Importance of Risk Analysis

- Conducted at least annually or when any major system or business change occurs
- Most health care organization haven't conducted risk analysis since security rule effective date
- Risk analysis reflects environmental, technical, business, etc. changes which don't stop

Importance of Risk Analysis

- Most health care organizations conduct qualitative or combined qualitative/ranking risk analysis
- Frequently risk analyses not standardized within organization
- Security controls evaluated often not technical
- Lack of follow through/mitigation an issue

Importance of Risk Analysis

- Organizations miss value – data collected during sound risk analysis applicability to other standards & processes
- Security officer – educational role
- Need to know business and assist in identifying risks to mitigate and risks to accept

Importance of Risk Analysis

- Balance identified risks between security, privacy & business needs
- Risk analysis should be globally rather than technically focused
- User involvement required – employees often know of risks before management
- Match perception with reality

Other Non-technical Requirements

- Risk management ties it all together
- Proper training key to successful security & privacy program
- Remote users represent significant non-technical threat
- Physical security – protect the infrastructure

Other Non-technical Requirements

- People most significant threat
- Role based access control – appropriate, tracked and enforced
- Trading partners & business associates – inter-organizational agreements/contracts
- Legal requirements (state, federal, case law)

Other Non-technical Requirements

- Security/privacy incident response
- Breach notification requirements
- Trust building between organizations and consumers
- Non-electronic data management
- Document/data retention & destruction (FRCP, HIPAA, etc.)

Selling Security

- ROI difficult to sell/demonstrate
- Package as insurance policy
- Identify damages caused by lax security
  - Regulatory compliance
  - Liability
  - Business reputation
  - Economic loss – trust, trade secrets, etc.
  - Lost data can bring down business

Selling Security

- Keep horror stories to a minimum
- Senior management – focus on non-technical risks (what will it cost in damages)
- Too much tech talk leads to glazed eyes
- Tie directly to business (must know the business)
- Clearly map to the risks (the value in pictures)

Selling Security

- Be reasonable – remember organization size, complexity and financial viability
- Sell phased security/privacy
- Rely on fact & accurate business impact
- Clearly spell out costs:
  - Solution cost (acquisition, installation, maintenance)
  - Staff support requirements (implementation & maintenance
- Be prepared to negotiate

Summary and Q&A

Chris Apgar, CISSP
President

10730 Southwest 62nd Place | Portland, Oregon 97219
503-977-9432 | 503-245-2626 Fax | www.ApgarAndAssoc.com