

Introducing HIPAA Security

Carol Richardson
Privacy Officer
Darren Lacey
Johns Hopkins
Chief Information Security Officer

HIPAA Security Rule

- Supports the Privacy Rule
- Applies to ePHI – Electronic Protected Health Information
- Final Rule issued in Feb. 2003
- Compliance due in April 2005
- Based on standard information security models (e.g. FIPS, NIST)

Security under HIPAA

- Process oriented – Required Parts
 - Risk Assessment
 - Risk Management
 - Documentation
 - Evaluation
- Specific controls – several of which are “addressable” (e.g. encryption, audits, etc.)

CIA² of Information Security

- Confidentiality – only authorized users access information
- Integrity – information accurately reflects input of authorized users only
- Availability – information can be accessed as needed by authorized users
- Accountability – attribution to users

Risk Management

- Threat environment
- System vulnerabilities
- Risk
- Primary controls
- Compensating controls
- Residual risk
- Evaluation

Controls

- Administrative
 - Workforce
 - Contingency planning
 - Business Associates
- Physical – facilities, workstations, device and media controls
- Technical –
 - Access control and authentication
 - Audit
 - Integrity
 - Transmission Security

How can an application or system be HIPAA Compliant?

- Defined by individual covered entities
- Expressed in policies and standards
- Security risks are documented and addressed
- Security controls are reasonable and appropriate
- When good controls are infeasible, compensating controls are implemented

What are the elements of a secure (i.e. HIPAA compliant) system?

- Authorization – administrative controls
- Authentication – preferably multi-factor, but at least strong passwords
- Data security – at the client, middleware and database
- Transmission security – for wireless this means encryption (e.g. WEP, SSL, VPN)
- Logging for audit purposes – access logs and a trace of user actions

Security and Safety

- Protecting privacy and confidentiality is often seen as an opposing value to patient care
- HIPAA security emphasizes many of the same values as in safety
 - Data integrity
 - Authorized access
 - Accountability
- We set a high bar for patient safety and good security contributes to safety

Steps for an institutional security program

- Inventory of systems and information assets
- Inventory of interfaces with other systems or risk environments
- Risk assessment and strategic plan
- Policies
- Standards and procedures
- Training for users and managers
- Implementing controls
- Periodic systems evaluation and monitoring

Concerns

- Circumvention
- Diversity of applications or systems
- Documentation of controls
- Systems accountability
- Audit logs and monitoring
- Transmission security – including email
- Risk assessment and management
- Incident response

Contacts

- Carol Richardson – Privacy
 - crichar@jhmi.edu or hipaa@jhmi.edu
- Darren Lacey – Security
 - dll@jhu.edu
- www.insidehopkinsmedicine.org/hipaa