Risk Analysis & Security Rule Compliance Activities

Marissa Gordon-Nguyen, JD, MPH
Health Information Privacy Specialist
HHS Office for Civil Rights
May 11, 2010
Security Rule Guidance Required By HITECH

• §13401(c) of the HITECH Act
• HHS must annually issue guidance on the most effective and appropriate technical safeguards for use in carrying out the Security Rule
• The Department must consult with stakeholders on the development of the annual guidance
Starting Point: Risk Analysis

- Risk Analysis
  - Administrative Safeguards
  - General Rules
    - Physical Safeguards
    - Technical Safeguards
Why is Risk Analysis Necessary for Compliance with the Security Rule?

45 CFR §164.308(a)(1)(ii)

• Covered entities must protect against:
  – **Reasonably anticipated** threats or hazards to the security/integrity of e-PHI they create, receive, maintain or transmit
  – **Reasonably anticipated** impermissible uses or disclosures

• Reduce risk to **reasonable and appropriate levels**

The risk analysis process determines what is “reasonable”
Reasonableness

Reasonably Anticipated Risks & Reasonable and Appropriate Security Measures: Unique to Each Organization

• Organizational Factors
  – Size
  – Complexity
  – Technical Infrastructure
  – Hardware
  – Software Security Capabilities
  – Cost of Security Measures

• External Factors
  – Natural environment
  – Regional infrastructure
  – Prevalence and sophistication of human threats (i.e., hacking)
The Risk Analysis Process: Key Activities Required by Security Rule

- **Evaluate** probability and criticality of potential risks
- **Adopt** reasonable and appropriate security safeguards based on results of risk analysis
- **Implement/Modify** security safeguards to reduce risks to a reasonable and appropriate level
- **Document** safeguards & rationale
- **Evaluate** effectiveness of measures in place
- **Maintain** continuous security protections
- **Repeat**
Risk Analysis Draft Guidance

• View the draft guidance on the OCR website at:
  http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule

• Share feedback at: OCRPrivacy@hhs.gov
  – Use subject line:
  • “Security Rule Guidance Comments”