HIPAA Security Essentials

Jennifer Cosey, President, Eagle Associates, Inc.
Financial Disclosure

• I have the following financial interests or relationships to disclose:
  o Eagle Associates, Inc.: Equity Owner
HIPAA Security

- Written Policies
- Sanctions
- Security Risk Analysis
- Technical Network Assessment
- Ransomware Response
- Staff Training
- Recognized Security Practices
Written Policies

- Administrative Safeguards
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Contingency Planning
- Physical Safeguards
- Technical Safeguards
- Security Incidents
Sanctions

• Impose sanctions whenever a workforce member commits a violation

• Apply sanctions equally

• Providers are not exempt
Security Risk Analysis

• Conduct a Security Risk Analysis at least annually

• Follow through on corrective actions/risk management

• Communicate issues found in SRA to appropriate staff
Security Risk Analysis Tool


- Windows only, not available for Mac systems
Technical Network Assessment

- Open port security
- User IDs
- Security patches and updates
- Password protocols
- Antivirus/firewall
- Automatic logoff
- Lockout protections
- Vulnerability scan
Ransomware Response

- Investigate
- Corrective Action
- Disciplinary action, if appropriate
- Short ransomware response procedure with which all staff are familiar
Staff Security Training

• Protection from malicious software
• Login monitoring
• Password management
• Periodic Security Reminders
Recognized Security Practices

- Amendment to Hitech Act in 2021
- Optional
- If implemented, mitigation of Civil Monetary Penalties for violations of Security Rule
- NIST Cybersecurity Framework
- Section 405d of Cybersecurity Act of 2015
- Must be able to show implementation for previous 12 months
- Must be implemented across entire organization