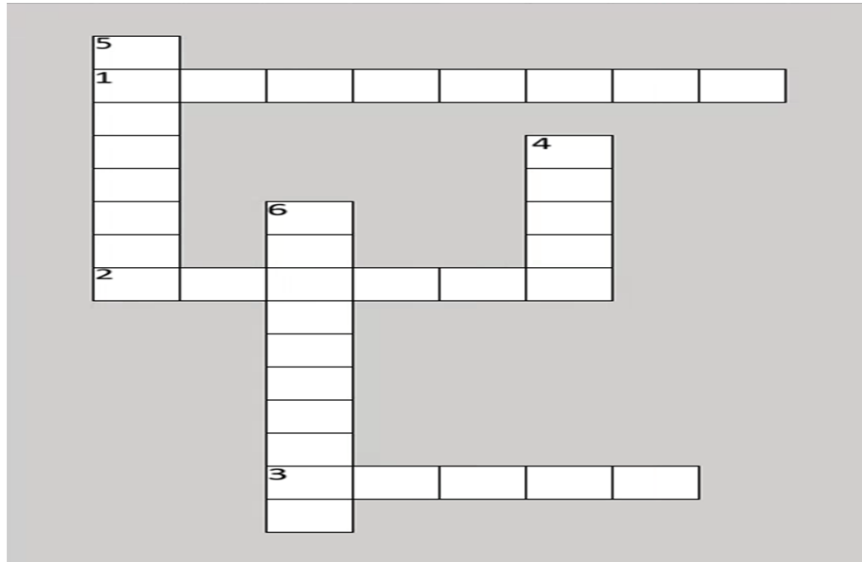




HIPAA Security  
North Carolina Public Health Association  
13-September-2016



HIPAA Security Clue 1: We want a SRA because it is \_\_\_\_\_.



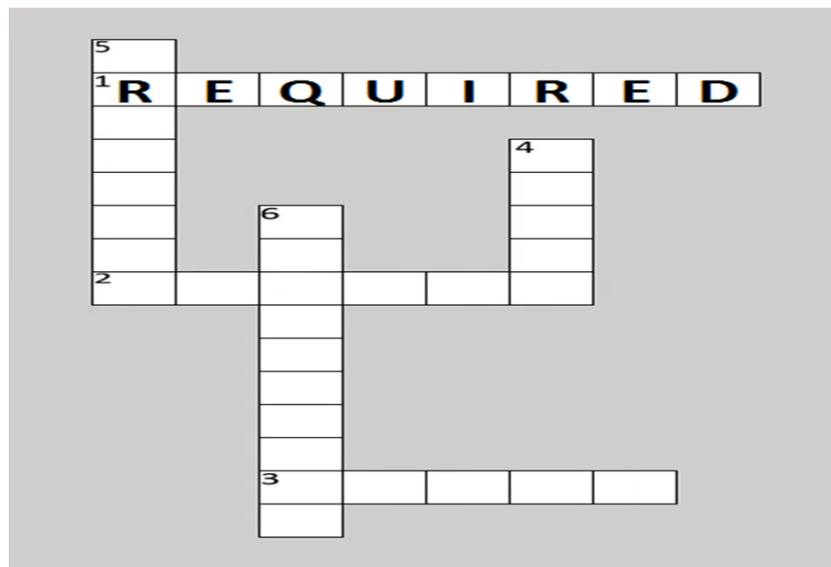
## Security Risk Assessment (SRA)

- The SRA helps the organization ensure it is **compliant** with HIPAA administrative, physical and technical safeguards
- The SRA is **required** by the HIPAA Security Rule
- Correspondingly, the SRA is **required** for attestation to CMS-Meaningful Use Stage 1 and 2



HIPAA Security Clue 2 – We need a SRA because our ePHI is a

-----.





## Security Risk Assessment (SRA)

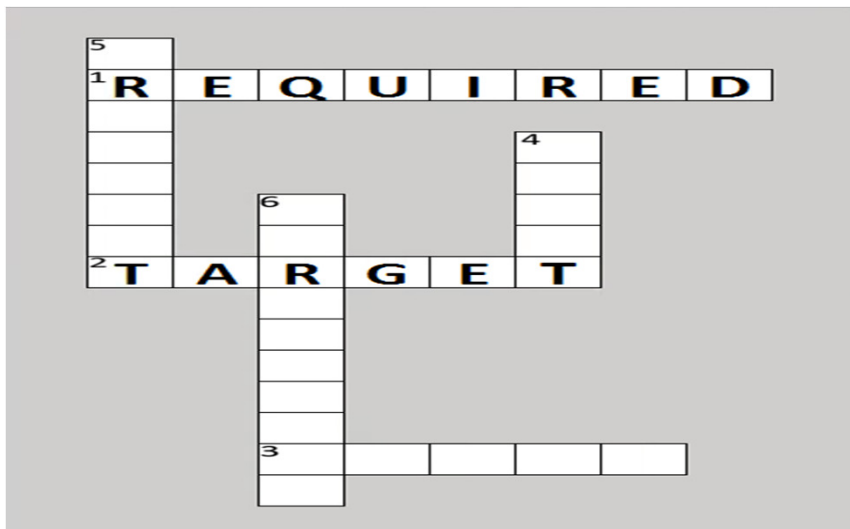
# Your ePHI is the target!


- Criminal attacks were the root cause in **50%** of ePHI data breach incidents. It was **45%** in 2015.
- Criminal attacks on covered entities and BAs has increased **125%** since 2011

Ponemon Institute 2015 and 2016 Benchmark Study on Privacy and Security of Healthcare Data

HIPAA Security Clue 3 – A breach of ePHI will result in loss of  
-----.





## HIPAA Security by the Numbers

- Black-Market Value: \$50/medical record – FBI
- 17,000 Patient Records Breached Per Day – HHS.gov
- Cost per Breached Record: \$188 – Ponemon
- HIPAA Penalties for a Lost Unencrypted Laptop: \$1.5M – OCR
- Loss of Patient Trust: 56% – Ponemon



## Compliance is **NOT** Security

- Comprehensive Audit Approach addresses ***five of the top five*** CIS Critical Security Controls (see [cisecurity.org](http://cisecurity.org))
- HealthIT Checklist ***partially*** addresses ***two of the top five*** CSCs



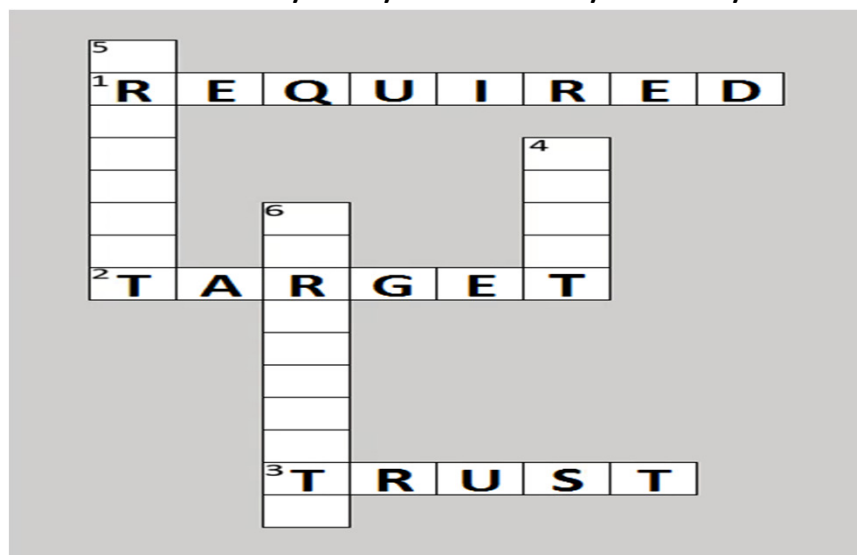
## Risky Thinking – “I can’t afford an audit-led SRA”

Can you afford a Breach?

- Single Loss Expectancy (SLE) = Asset Value or Fines x **Exposure Factor**
- Annualized Loss Expectancy = SLE x Annual Rate of Occurrence
  - Checklist ALE (one incident) = \$50K x 45% = \$22.5K
  - Audit Guided ALE (one incident) = \$5K x 45% = \$2.25K



HIPAA Security Clue 4 – Employing an \_\_\_\_\_ approach to the assessment is the best way to systematically identify locations of ePHI.



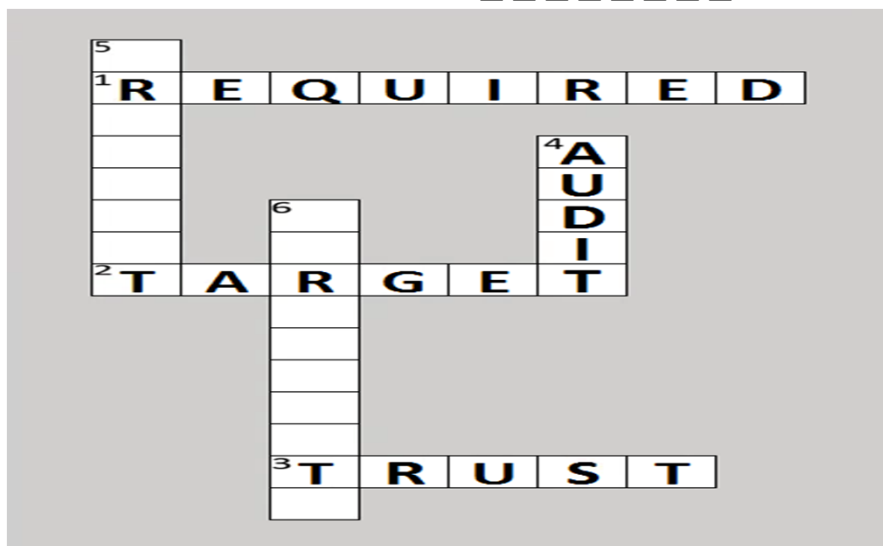
## Carolinas IT SRA Approach

*The Goal: to reveal the areas where your ePHI is at risk and recommend steps to reduce that risk*

- Diagnostic Tools (vulnerability, AD scans)
- Checklists
- Professional Reports
- Guided by an ISACA Certified Information Systems Auditor
- Customized to your organization



HIPAA Security Clue 5 – Security training is required annually, but it should be more \_\_\_\_\_.

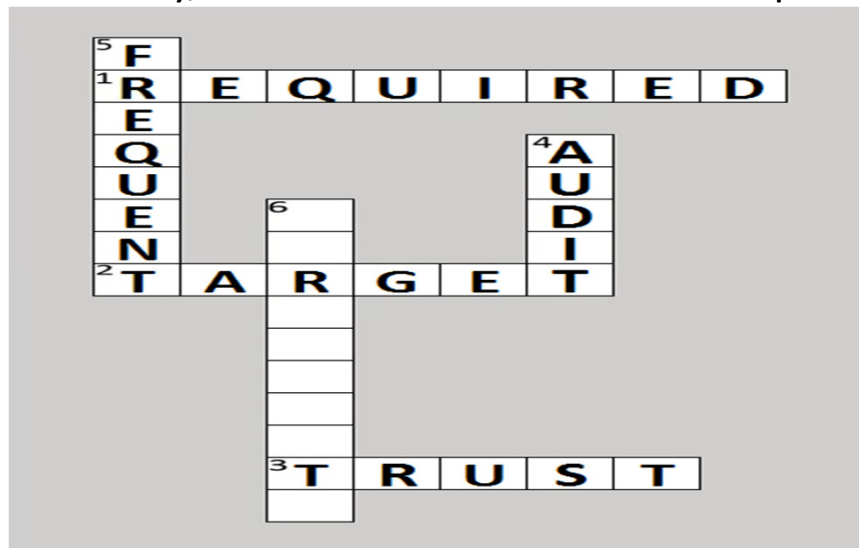


## Common Vulnerabilities

- Lack of or weak password controls
- Poor management of user accounts/generic accounts
- No automatic logoff/session timeout
- Lack of HIPAA Security specific policies and training
- Inadequate controls for email, encryption
- Misconfiguration of Firewall/Intrusion Protection (IDS/IPS)
- Poor management of BAAs



HIPAA Security Clue 6 – Business Associate \_\_\_\_\_ are a necessity, but there are several misconceptions.

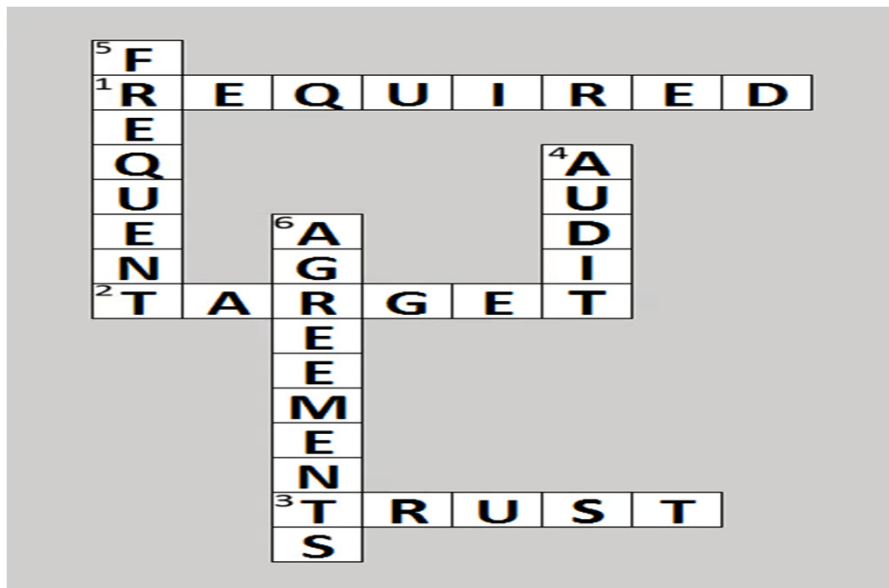


## BAA Myths

- We don't need a BAA if the business associate never actually looks at the data
- We have less risk with the BAA
- Having a signed BAA is all we need to do to ensure the business associate is HIPAA compliant (audit and subcontractors)
- All BAAs are the same



## Congratulations!





***Thank You!***

**R. Greg Manson**

**Director of Audit and Compliance**

**[Greg.Manson@CarolinasIT.com](mailto:Greg.Manson@CarolinasIT.com), 919-573-4084**

1600 Hillsborough Street  
Raleigh, NC 27605  
[www.CarolinasIT.com](http://www.CarolinasIT.com)

