What to expect from a HIPAA Security Risk Assessment (SRA)

Kevin Atkins, CAHIMS

Director

Dakota State University

Center for the Advancement of Health IT / HealthPOINT

QPP-SURS

For more information

www.telligenqpp.com

Objectives

Discuss HIPAA Requirements for a SRA

Define what constitutes a Risk

Identify the elements of a SRA

Origins of Security Risk Assessment

HIPAA Security Rule

Proposed in 1998……..….Enacted in 2003

Mandatory in 2006

45 CFR (Code of Federal Regulations) Part 160

Subparts A & C of Part 164 (164.302 – 318)

Health Information Technology for Economic and Clinical (HITECH) Act

Office for Civil Rights (OCR) responsible for guidance and enforcement

Definitions

Vulnerability

A flaw or weakness in **system security procedures, design, implementation, or internal controls** that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

Breach

Impermissible use or disclosure that compromises the security or privacy of protected health information (PHI).

Threat

The potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

- Natural (floods, earthquakes, tornadoes)
- Human (hacking, unauthorized access)
- Environmental (power failure, chemicals, pollution)

Definitions, cont.

Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

(https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final)

In other words

Risk is a function of:

(1) The likelihood of a given threat triggering or exploiting a vulnerability

(2) The resulting impact on the organization

Definitions, cont.

Standard

- The “What”
- Must comply with every “standard”

Implementation Specification

- The “How”
  - Required – must be implemented
  - Addressable – not optional

B O R I N G!!!

Purpose of Security Rule

Establishes national standards to protect Electronic Protected Health Information (EPHI)

Requires Administrative, Physical, Technical Safeguards
- Confidentiality, Integrity, Security

Privacy Rule vs Security Rule
- Privacy Rule: all PHI
- Security Rule: **ELECTRONIC** PHI

Requires entities to
- Evaluate risks and vulnerabilities
- Implement reasonable and appropriate security measures

Requirements

Security Management Process (Standard)

164.308(a)(1)(i)

Implement policies and procedures to prevent, detect, contain, and correct security violations.

Four required Implementation Specifications

164.308(a)(1)(ii)(A) (Implementation Specification)

Risk Analysis: conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

Qualitative vs Quantitative

Qualitative Assessment

- Cons: Subjective, value of loss not quantified
- Pros: More common, quicker to complete, focus is on understanding the risk

Quantitative Assessment

- Cons: Exhaustive, costly, time-consuming
- Pros: Identify greatest risk based on financial impact

Qualitative & Quantitative tools

Qualitative

Delphi Technique: risk brainstorming – identify, analyze, evaluate risk on individual and anonymous basis.

Structured What-If Technique (SWIFT): team-based approach – uses "What If" considerations.

https://www.project-risk-manager.com/blog/qualitative-risk-techniques/

Quantitative

Financial sector, chemical process industry, explosives industry (Wikipedia)

https://en.wikipedia.org/wiki/Quantitative_risk_assessment_software

CAHIT: hybrid approach - qualitative on the front end, quantitative on back end; quantitative algorithm can be overridden in final report (subjectivity coming into play).

Elements of an SRA
Scope

Includes **ALL** potential risks and vulnerabilities to the confidentiality, availability and integrity of **ALL** EPHI that an organization creates, receives, maintains, or transmits.

REMEMBER **EPHI IS more than medical records**

Billing information Appointment information

Insurance claims Reports Network shares

What am I forgetting?

1

Type : X-ray Scanner **Document :** ePHI **Vendor :** Solcom
Location : Scanning area **Used/Disclosed By :** scanning staff **Hardware/Service :** Scanner/workstation
Safeguards in place : Physical facility and user access controls
Vulnerabilities : Destruction or closure of the facility, loss of equipment, records and data
Threats : Natural and man-made disasters, standard network threats
Likelihood : Low **Criticality :** Low **Impact :** HIPAA Breach, Fines

2

Type : AS 400 Server **Document :** ePHI **Vendor :** IBM
Location : server room **Used/Disclosed By :** all staff **Hardware/Service :** AS 400
Safeguards in place : Physical facility and user access controls; UPS, HVAC, badge reader lock; server will perform a safe shutdown when temp
Vulnerabilities : Destruction or closure of the facility, loss of PHI equipment, records, water based fire suppression system
Threats : Natural and man-made disasters, standard network threats, removal of device without removal of ePHI
Likelihood : Low **Criticality :** High **Impact :** HIPAA Breach, Fines

3

Type : Legacy server **Document :** ePHI **Vendor :** IBM
Location : basement **Used/Disclosed By :** IT **Hardware/Service :** iSeries AS400
Safeguards in place : Physical facility, and user access controls, locked room with key card access,
Vulnerabilities : Destruction or closure of the facility, loss of PHI equipment, records and data, data is unecrypted.
Threats : Natural and man-made disasters, standard network threats, removal of device without removal of ePHI
Likelihood : Low **Criticality :** Low **Impact :** HIPAA Breach, Fines

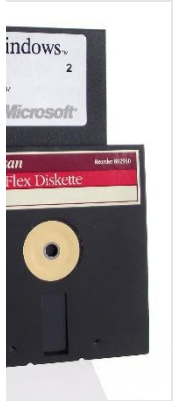
4

Type : Network copiers/fax/scanners/printers **Document :** potential ePHI **Vendor :** various
Location : throughout the facility **Used/Disclosed By :** All staff **Hardware/Service :**
Safeguards in place : Administrative safeguards, Physical access controls
Vulnerabilities : Destruction or closure of the facility, loss of PHI equipment, records and data;
Threats : Natural and man-made disasters; removing from facility without proper removal of ePHI
Likelihood : Low **Criticality :** Low **Impact :** Security Best Practices

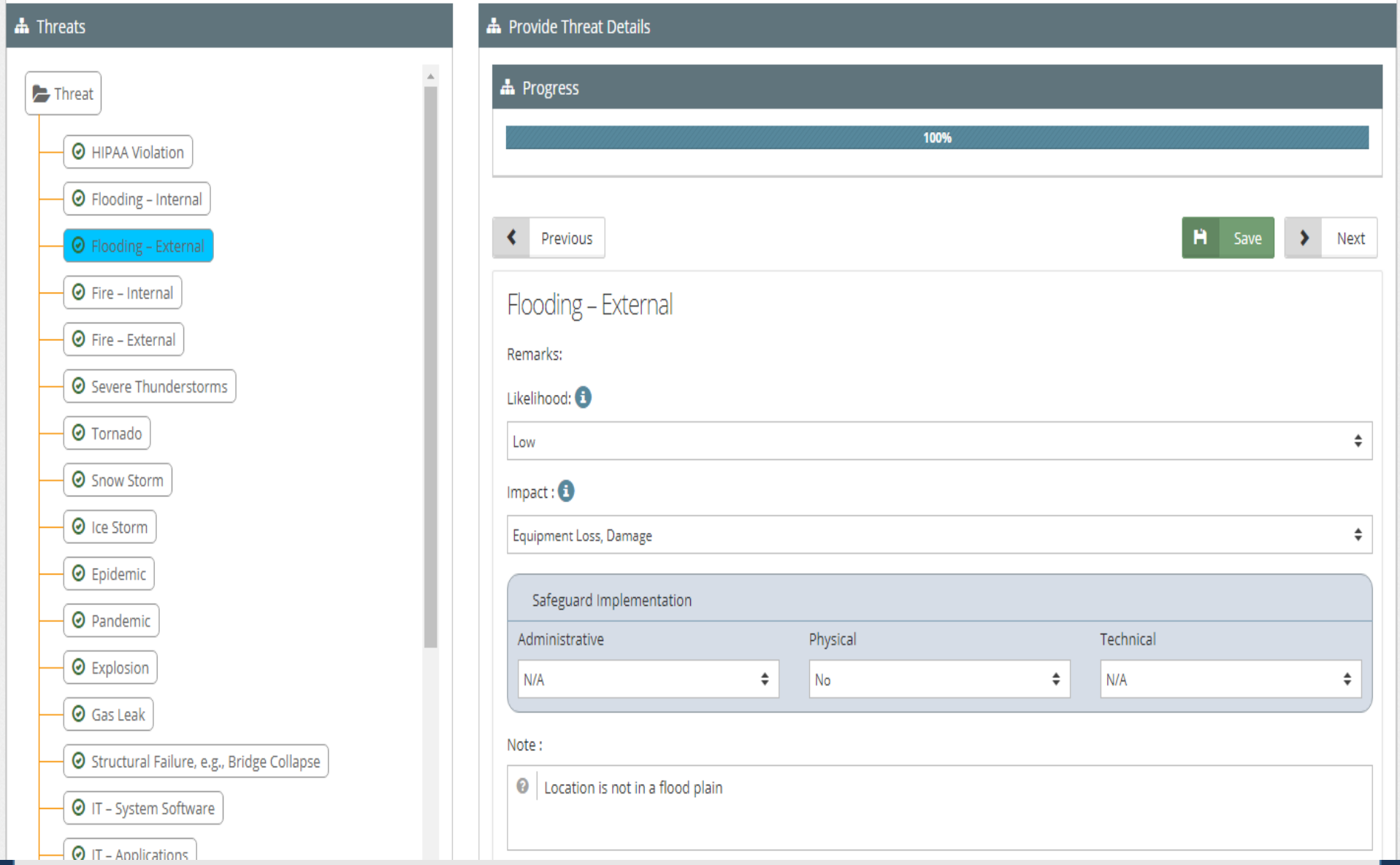
5

Type : Onsite Backups **Document :** backup copies of ePHI **Vendor :** IBM
Location : fire proof safe within server room **Used/Disclosed By :** IT **Hardware/Service :** BRMS/VEEAM tape backups
Safeguards in place : Physical facility and user access controls; UPS, HVAC, fire suppression system, kept in fire-proof safe; badge reader lock;
Vulnerabilities : Destruction or closure of the facility, loss of PHI equipment, records and data; backups kept on-site are not encrypted
Threats : Natural and man-made disasters
Likelihood : Low **Criticality :** Low **Impact :** HIPAA Breach, Fines

Where to look for EPHI



Elements of an SRA



Elements of an SRA
Business Associates

What are they?

Person or Organization that Creates, Accesses, Transmits, or Stores EPHI on your behalf.

- Coders or Coding companies
- Backup storage vendors

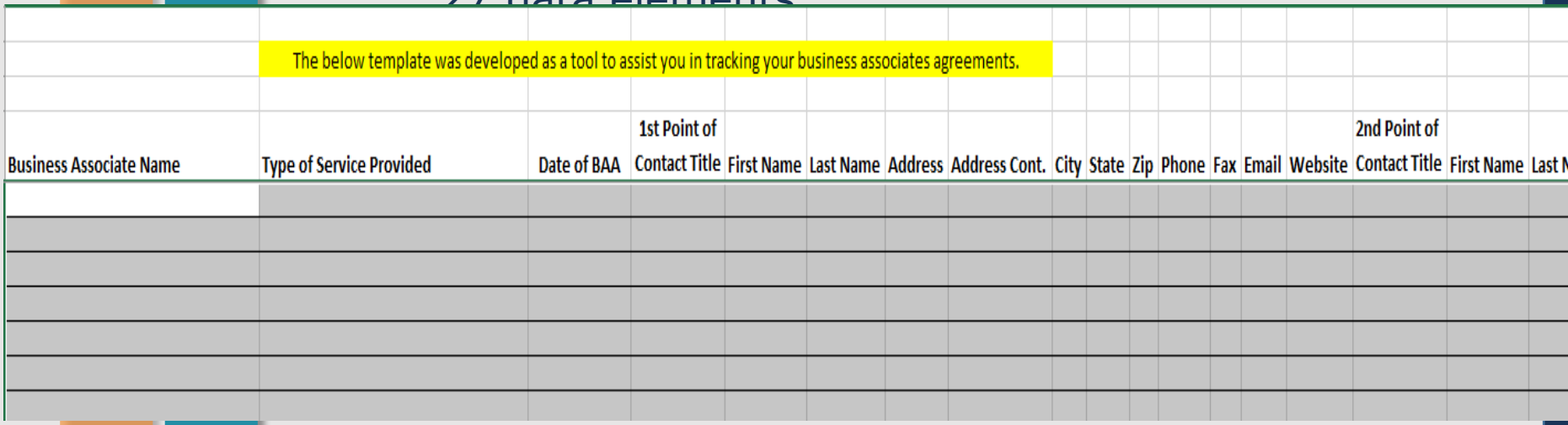
Anyone not employed by you, working with your EPHI

Elements of an SRA
Business Associate Agreements

Business Associates were (are) a focus of OCR during Phase II audits

OCR requested specific information

- 27 data elements



The below template was developed as a tool to assist you in tracking your business associates agreements.

Business Associate Name	Type of Service Provided	Date of BAA	1st Point of Contact Title	First Name	Last Name	Address	Address Cont.	City	State	Zip	Phone	Fax	Email	Website	2nd Point of Contact Title	First Name	Last N

NOT downloadable. Email me for a copy! ☺

Citation : §164.308(a)(1)(i) | Review Risk Analysis

Skip | Flag

Does your practice have a process for periodically reviewing its risk analysis policies and procedures and making updates as necessary?

Safeguard Examples | Things To Consider | Threat and Vulnerability

Implement policies and procedures to prevent, detect, contain, and correct security violations. [45 CFR §164.308(a)(1)(i)] Review and update the current risk assessment policy and procedures to adapt your security program to changing needs. [NIST SP 800-53 RA-1]

(•) Yes ( ) Partial ( ) No

Likelihood :

Medium

Impact :

Security Best Practices

Current Activities :

Current Activities

Safeguard Implementation

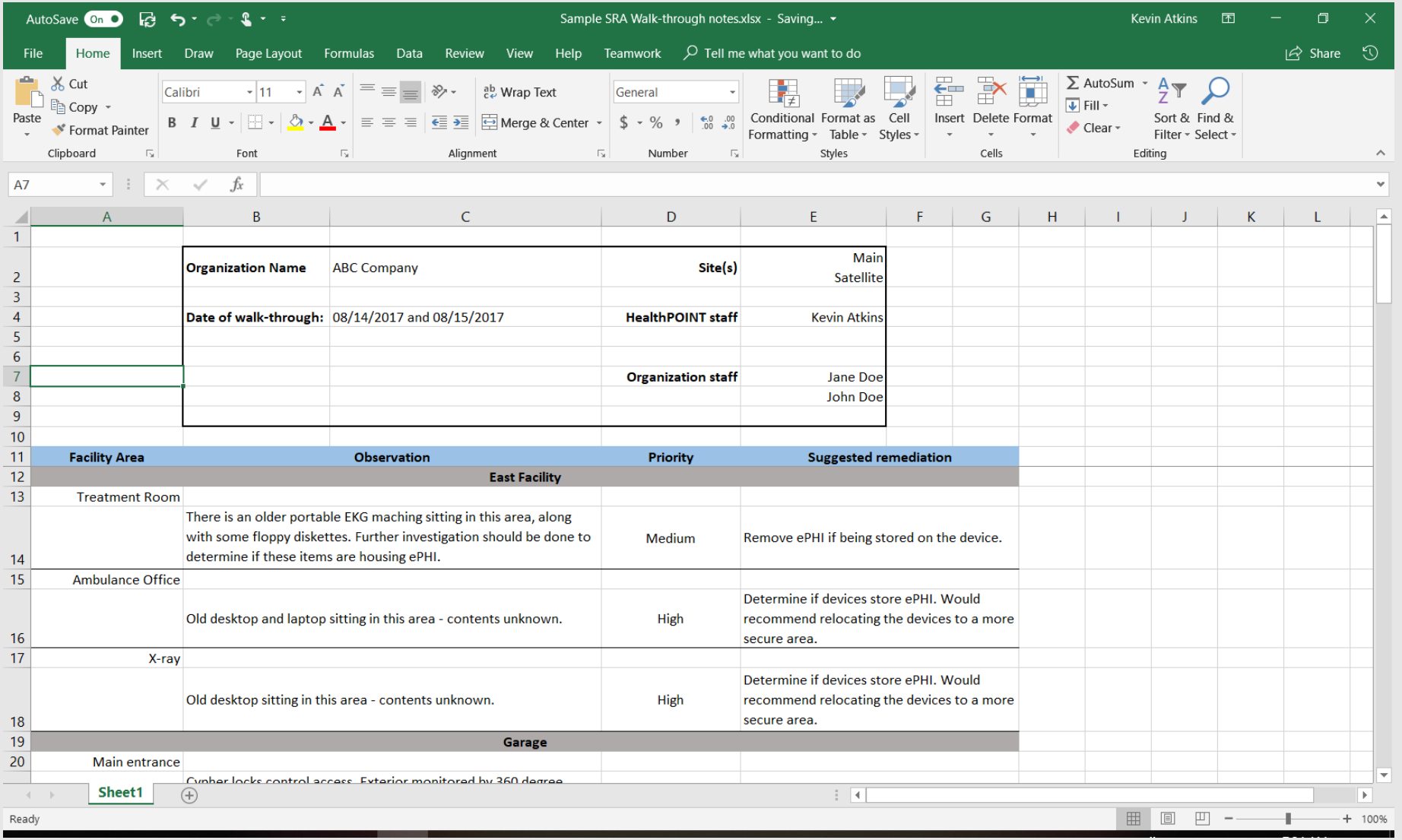
Administrative	Physical	Technical
Yes	N/A	N/A

Note :

Notes for answer

Files

Elements of an SRA Walk Through



Elements of an SRA Report

A deliverable of ANY SRA should be a final report.

- Presents/summarizes results
- Used to guide/prioritize remediation

FINAL SRA Report

Summary

A Risk Assessment

Designed to aid you in protecting the confidentiality, integrity, and availability of ePHI

May be required for Medicare and Medicaid incentive payment programs (i.e. MIPS, etc.)

Many methods available (consultant, checklist – (ill advised), online tool - www.healthit.gov)

EPHI IS MORE THAN JUST THE EHR!!

The End

THANK YOU

Kevin Atkins, CAHIMS

Director

Dakota State University Center for the Advancement of Health IT

Kevin.Atkins@dsu.edu