HIPAA Security Risk Assessment (SRA)

Dan Friedrich, CISSP

Director, Center for Advancement of Health IT Dakota State University

healthPOINT at Dakota State University | SECURITY services

Telligen® Healthcare Intelligence

DSU DAKOTA STATE

Objectives

Discuss QPP and HIPAA Requirements for a SRA

Define what constitutes a Risk

Identify the elements of a SRA

SRA and the Quality Payment Program

healthPOINT at Dakota State University | SECURITY services

QPP Resource Center

Telligen® Healthcare Intelligence

DSU DAKOTA STATE

Required by Promoting Interoperability

- https://qpp.cms.gov/docs/pi_specifications/Transition%20Measure%20Specifications/2018.MIPS%20ACI%20Transition%20Measure_Security%20Risk%20Analysis.pdf

- Required for Base Score: Yes
- Percentage of Performance Score: N/A
- Eligible for Bonus Score: No

Note: MIPS eligible clinicians must fulfill the requirements of base score measures to earn a base score in order to earn any score in the Advancing Care Information performance category. In addition to the base score, eligible clinicians have the opportunity to earn additional credit through the submission of performance measures and a bonus measure and/or activity.

Timing for QPP

- It is acceptable for the security risk analysis to be conducted outside the MIPS performance period;
- the analysis must be unique for each MIPS performance period,
- the scope must include the full MIPS performance period,
- and must be conducted within the calendar year of the MIPS performance period (January 1st – December 31st).

SRA and the Quality Payment Program

Objective: Protect Patient Health Information

Measure: Security Risk Analysis

Conduct or review a security risk analysis in accordance with the requirements in 45 CFR 164.308(a)(1), including addressing the security (to include encryption) of ePHI data created or maintained by certified electronic health record technology (CEHRT) in accordance with requirements in 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the MIPS eligible clinician's risk management process.

Measure ID: ACI_TRANS_PPHI_1

healthPOINT at Dakota State University | SECURITY services

Telligen® Healthcare Intelligence

DSU DAKOTA STATE

SRA and the Quality Payment Program

Conduct or review a security risk analysis in accordance with the requirements in 45 CFR 164.308(a)(1),

including addressing the security (to include encryption) of ePHI data created or maintained by certified electronic health record technology (CEHRT)

SRA and the Quality Payment Program

in accordance with requirements in 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3),

(iv)*Encryption and decryption (Addressable).* Implement a mechanism to encrypt and decrypt electronic protected health information.

- **(3)** When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressableimplementation specifications, a covered entity or business associate must -
- **(i)** Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and
- **(ii)** As applicable to the covered entity or business associate -
- **(A)** Implement the implementation specification if reasonable and appropriate; or
- **(B)** If implementing the implementation specification is not reasonable and appropriate -
- $(*1*) Document why it would not be reasonable and appropriate to implement the implementation specification; and
- $(*2*) Implement an equivalent alternative measure if reasonable and appropriate.

Addressable ≠ Optional

healthPOINT at Dakota State University | SECURITY services

QPP Resource Center

Telligen® Healthcare Intelligence

DSU DAKOTA STATE

SRA and the Quality Payment Program

And finally

implement security updates as necessary and correct identified security deficiencies as part of the MIPS eligible clinician's risk management process.

SRA and the Quality Payment Program

Objective: Protect Patient Health Information

Measure: Security Risk Analysis

Conduct or review a security risk analysis in accordance with the requirements in 45 CFR 164.308(a)(1), including addressing the security (to include encryption) of ePHI data created or maintained by certified electronic health record technology (CEHRT) in accordance with requirements in 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the MIPS eligible clinician's risk management process.

Measure ID: ACI_TRANS_PPHI_1

HIPAA SRA Requirements

164.308(a)(1)(ii)(A)

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.

Assessment VS Mitigation

• Assessment

- Identify assets
- Identify specific threats to those assets
- Provide some way of prioritizing
- Help determine residual risk
  - Reduce
  - Transfer
  - Accept
  - Reject

• Mitigation

- Efforts to reduce or eliminate
  - Probability
  - Severity
- Of a threat
  - HIPAA/HITECH Security Checklist
  - NIST 800-53
  - Others

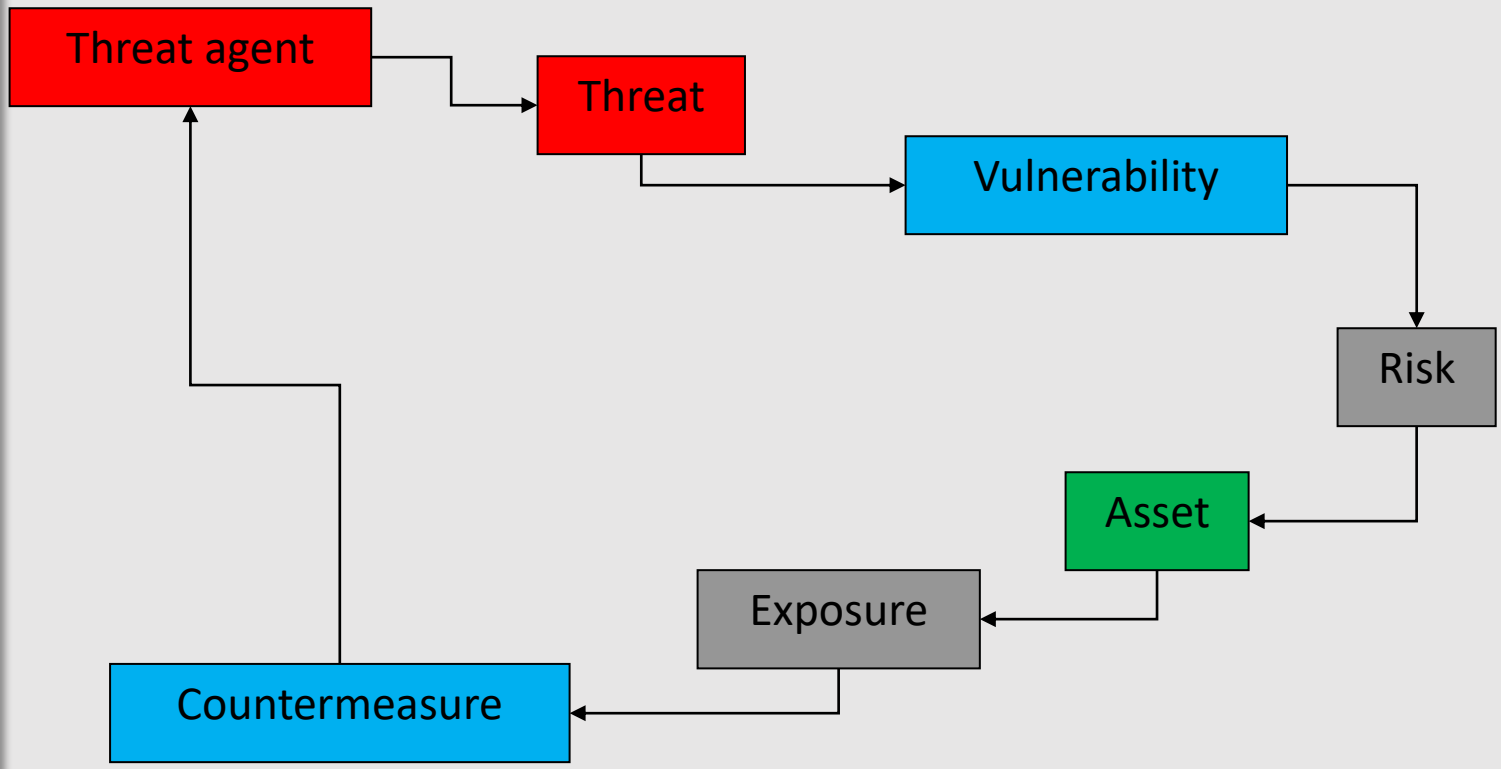
healthPOINT at Dakota State University | SECURITY services

Telligen®
Healthcare Intelligence

DSU DAKOTA STATE

The Threat Relationship

- Can't Control Can Control Must Understand



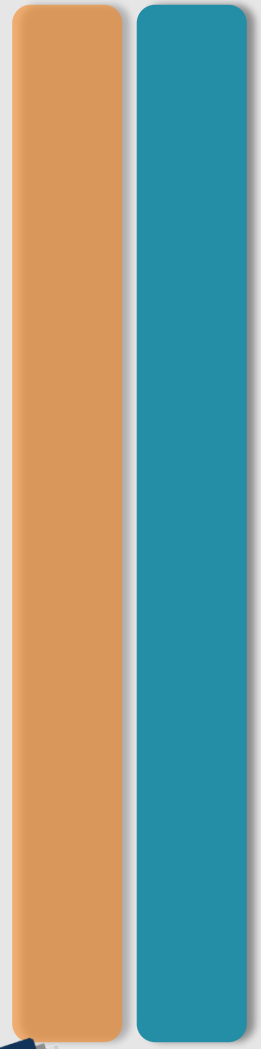
healthPOINT at Dakota State University | SECURITY services

QPP Resource Center

Telligen® Healthcare Intelligence

DSU DAKOTA STATE

Qualitative vs Quantitative



Quantitative Assessment

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

Qualitative Assessment

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

Hybrid

healthPOINT at Dakota State University | SECURITY services

QPP Resource Center

Telligen® Healthcare Intelligence

DSU DAKOTA STATE

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.

Quantitative

Less often used in Healthcare.

Financial sector, chemical process industry, explosives industry

healthPOINT at Dakota State University | SECURITY services

QPP Resource Center

Telligen® Healthcare Intelligence

DSU DAKOTA STATE

Security Risk Assessment Scope

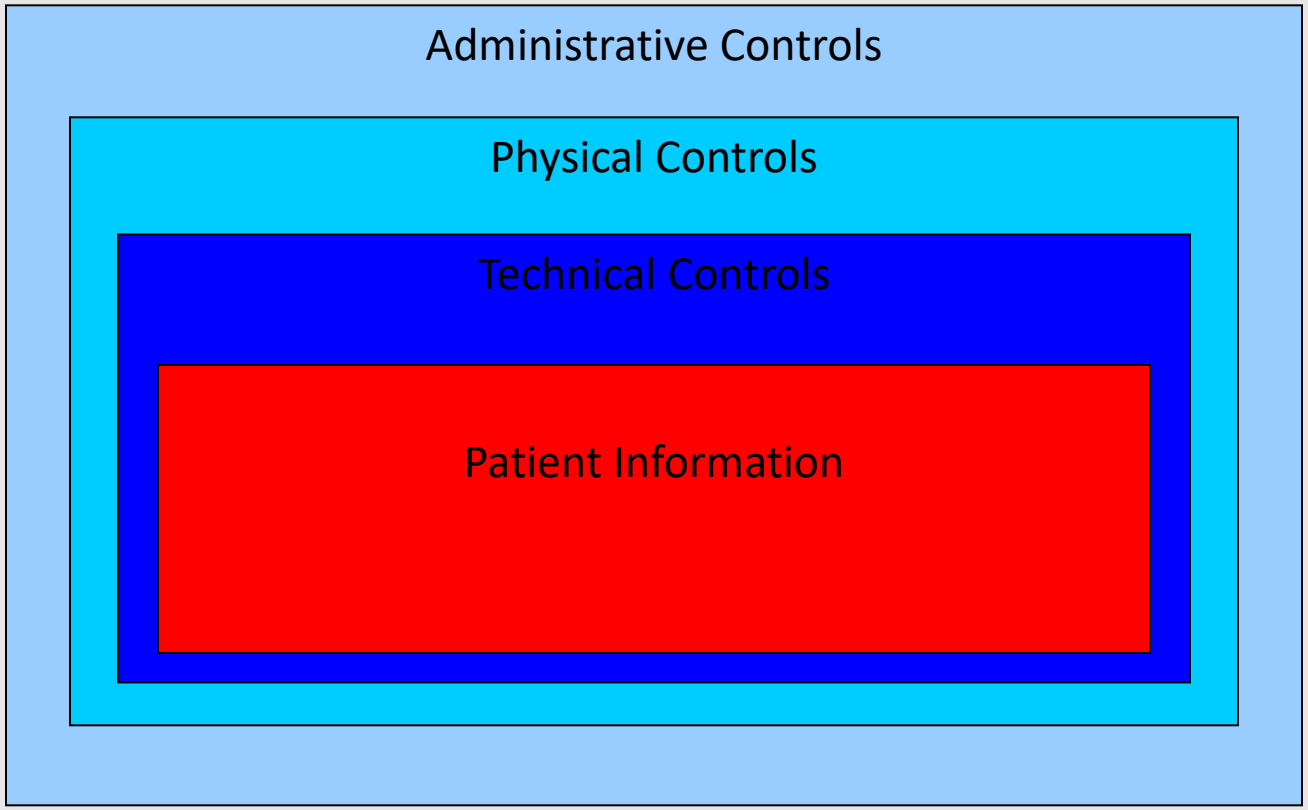
Includes potential risks and vulnerabilities to the confidentiality, availability and integrity of **ALL** EPHI that an organization creates, receives, maintains, or transmits. [164.306(a)]

REMEMBER **EPHI IS more than medical records**

Billing information Appointment information
Insurance claims information Reports

What am I forgetting?

Risk Assessment Perspective



healthPOINT at Dakota State University | SECURITY services

QPP Resource Center

Telligen® Healthcare Intelligence

DSU DAKOTA STATE

Where to look for EPHI

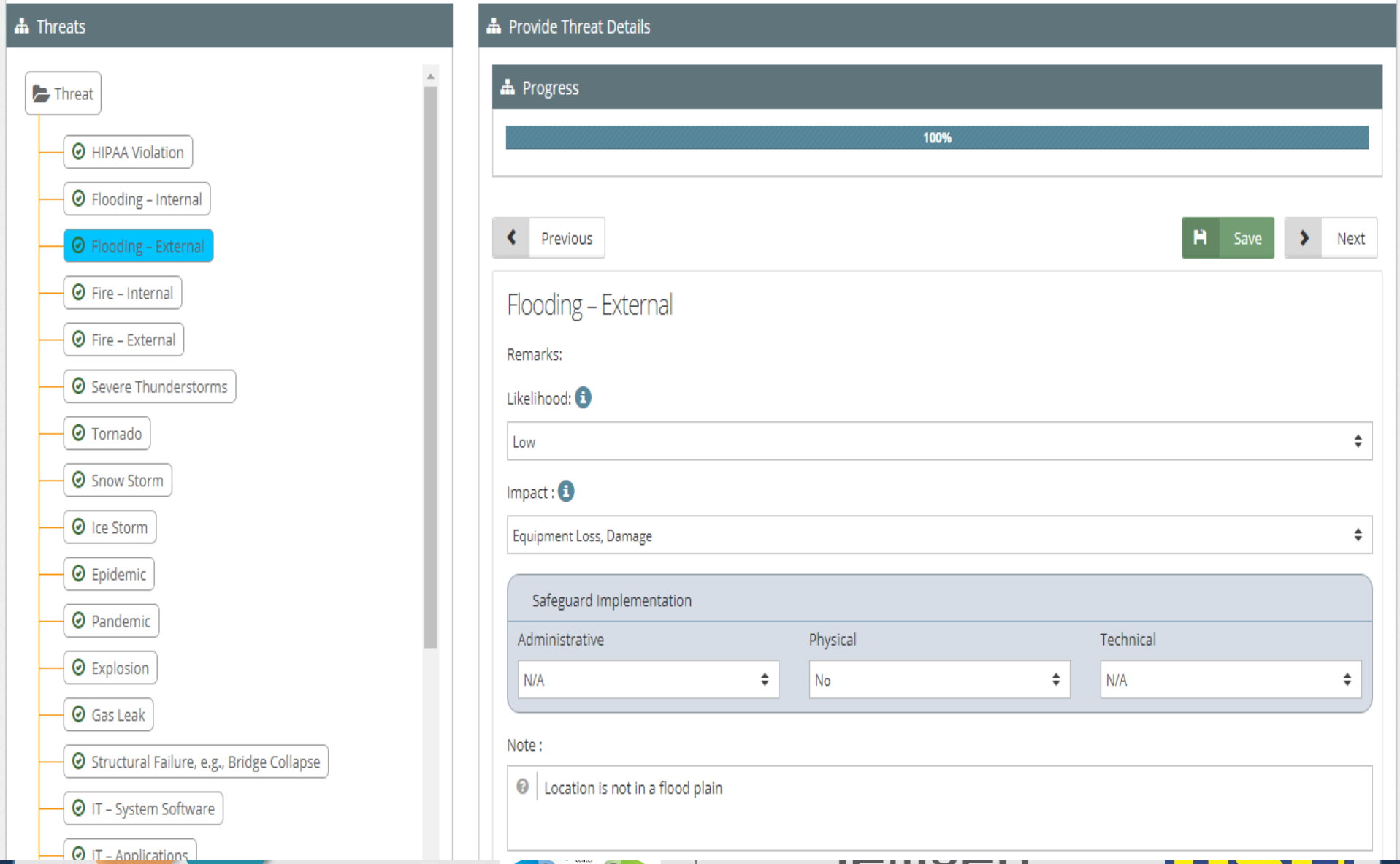
healthPOINT at Dakota State University | SECURITY services

QPP Resource Center

Telligen® Healthcare Intelligence

DSU DAKOTA STATE

Elements of a Security Risk Assessment



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

Document Business Associate Agreements

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

OCR requested specific information

- 27 data elements
- Business Associate Name, type of service,

Questions?

healthPOINT at Dakota State University | SECURITY services

QPP Resource Center

Telligen® Healthcare Intelligence

DSU DAKOTA STATE

THANK YOU

Dan Friedrich, CISSP

Director, Center for the Advancement of Health IT

Dakota State University

Dan.Friedrich@dsu.edu

(605) 256 5555

healthPOINT at Dakota State University | SECURITY services

QPP Resource Center

Telligen® Healthcare Intelligence

DSU DAKOTA STATE