HIPAA Critical Updates Workshop
September 13, 2016

Helpful Hints for Completing HealthIT.gov Security Risk Analysis Tool

Overview

"The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that covered entities conduct a risk assessment of their healthcare organization. A risk assessment helps your organization ensure it is compliant with HIPAA's administrative, physical, and technical safeguards. A risk assessment also helps reveal areas where your organization's protected health information (PHI) could be at risk. Watch the Security Risk Analysis (SRA) video to learn more about the assessment process and how it benefits your organization or visit the Office for Civil Rights' official guidance (http://www.hhs.gov/hipaa/for-professionals/security/guidance/final-guidance-risk-analysis/index.html)."

Important Links

1. Main SRA Site
https://www.healthit.gov/providers-professionals/ehr-privacy-security

2. Application Download
https://www.healthit.gov/providers-professionals/security-risk-assessment-tool

3. Videos
https://www.healthit.gov/providers-professionals/security-risk-assessment-videos
   - Security 101: Security Risk Analysis
   - Security 101: Contingency Planning
   - SRA Tool Tutorial

4. SRA is also in the form of a manual that can be downloaded and/or printed. It would be more tedious to complete the analysis this way but it is helpful, especially when sitting down with your agency's IT dept.

5. Keep in mind these key elements:
   - Scope of risk analysis must cover all the ePHI that organization creates, receives, maintains or transmits, includes all forms of electronic media (hard drives, laptops, backup tapes, smart cards, other forms of electronic media)
   - Includes electronic material, information technology physically in the office, and information stored or accessed remotely
   - Includes appointments, billing, and insurance claims

Things to have on hand before starting the SRA tool

1. Privacy and Security Policies and Procedures
2. A list documenting where ePHI is stored (inventory of all information systems including components, hardware, and software that compromise them)
3. A list documenting where ePHI flows (i.e. to patient, to another provider, to offsite server or back up facility)
4. A list documenting how ePHI is shared or transmitted (i.e. email, fax, shared network drives, health information exchange)
5. A list of the agency's Business Associates (information needed includes: BA name, type, and address) (for definition of business associates, see the OCR website)

6. Identify and document possible threats and vulnerabilities
    a. Threat examples: hackers, natural disasters, power outages
    b. Vulnerability examples: unencrypted laptops, failure to follow policies and procedures, lack of physical safeguards to computer workstations
7. Identify and document current security measures in place (administrative, technical, and physical) – will require collaboration with the agency's Information Technology Department
8. Determine the likelihood and impact of potential threats as low, medium or high
9. Document a list of corrective actions to mitigate the risks. Corrective actions could include:
    a) Putting a new policy in place
    b) Training staff on a new process
    c) Adding physical safeguards, such as locks on doors

<u>Tips about completing the tool</u>

1. More than one person can have a login and you can divide the sections
2. Can log in and out as many times as needed and your information will be saved. Can also access the navigator button to select a specific section
3. Before login to start the assessment, you need to complete the tabs, "Users," "About Your Practice," "Business Associates," and Asset Inventory."
    a. <u>Business Associates Tab</u>
        - Each time you want to add a BA, click on the tab "Business Associates" again
    b. <u>Asset Inventory Tab</u>
        - 4 fields to complete 1) name, 2) type, 3) has ePHI, 4) assignee
        - Example: 1) EHR Patagonia, 2) An application – provider enters data or machine stores the ePHI, 3) document whether asset receives, stores, or transmits ePHI, 4) document who in organization is responsible for the asset
4. Start discussions with your IT Department before attempting to complete the tool
    a. Discuss which department will complete the analysis and how remediation will be handled
5. Begin by reviewing the videos on the HealthIT.gov website (allow approx. 25 to 30 minutes for all 3 videos)
6. Proceed through the tool to answer questions capable of answering and to document questions will need IT or another department to answer (first review and attempt to complete took 2 hours but did not include documentation of remediation plans)
    a. In the tool, you can document the answers, notes to self and remediation plans
    b. Includes mechanism to flag questions that still need answered or require input from IT or another department
    c. After first attempt at the tool, met with IT Department's designated SRA representative and did the following:
        i. Reviewed the SRA manual and electronic tool together
        ii. Identified questions which neither department knew the answer
        iii. Privacy Officer agreed to go through the tool again and give IT batches of questions to research and answer if possible

Resources

1. ONC Privacy and Security Resources on Health IT
2. HHS Office for Civil Rights: Health Information Privacy Resources
3. EHR Incentives and Certifications: Meaningful Use
4. NIST Special Publication 800-66, Revision 1: An Introductory Resource Guide for Implementing the HIPAA Security Rule
5. NIST Special Publication 800-30, Revision 1: Guide for Conducting Risk Assessments
6. http://www.medscape.org/sites/advances/patients-rights

Submitted by Carla Julian, Orange County Health Department Privacy Officer