CORE BANK

Healthcare Banking Bulletin

Issue 8 - October 28, 2022

Annual Requirements: Security Risk Assessments

Did you know that the Departments of Health and Human Services require covered entities to perform an annual Security Risk Assessment (SRA) to assess potential threats and vulnerabilities? There are often a lot of misconceptions around SRAs which lead quickly to noncompliance. This article will address some of the most common misconceptions around SRAs.

SRA Facts

- If you are a covered entity, you are required to perform this assessment every year.
- This requirement is not satisfied merely by having a certified EHR
- Failure to comply can result in fines or loss of incentive payments
- Outsourcing an SRA is not required, this can be done in-house
- Relying on the IT support at your EHR vendor to 'have it covered' is insufficient
- You do not need to fully re-evaluate every section of the SRA every year
- There are free tools available to help you stay in compliance

One of the best things you can do to structure ongoing compliance is to dedicate a timeframe every year to complete your SRA. Ideally, aim to complete your SRA in advance of your annual budgeting processes to leave funds for remediation resources if needed. For example, your assessment may uncover that you need to upgrade software, purchase additional insurance, or add security cameras to the physical location to reduce risks to your facility. The more time you grant yourself between your SRA and your budget, the more time you have to assess risk and financial impact while planning for timely implementation.

SRA Tool

HHS has a great tool to help walk you through your SRA, you can access that tool here: https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool.

AUTHORED BY:

Taya Gordon, EMBA, CMPE, CMOM

LinkedIn: https://www.linkedin.com/in/tayagordon/

Twitter: https://twitter.com/tayamoheiser

Most of it is pretty straightforward but in addition the Office of the National Coordinator and the Office of Civil Rights has put together education and training to help guide users on how to use this tool which you can access here: https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html.

The reason for providing both an SRA tool and comprehensive training is two-fold: (1) HHS wants to support organizations in remaining compliance and achieving security success and (2) they want to make sure you have no argument for non-compliance with this requirement.

Performing an SRA gives you valuable information with which you can proactively prepare your organization against threats whether they are physical, administrative, or technological in nature. With the continued rise of cyberattacks and patient information held hostage for ransom, we have to make every effort to protect the integrity and security of our patients' information. As ransomware attacks and payouts increase, insurance to help cover the losses of ransomware is becoming more challenging to obtain. Performance of annual SRAs with documented progress and risk remediation may help you to secure a cyber insurance policy or at the very least to prove that your facility was not negligent in its responsibility to protect patient information.

The first time you perform an SRA it can seem very daunting, every time you change a significant piece of software (like the Electronic Health Record) and have to do an SRA it can feel overwhelming. Regardless, this process is undoubtedly worth your time. Even if this wasn't a requirement it would be strongly recommended by industry experts because even a seemingly small breach can create enough strife and financial devastation to force practice closure.

Take the time to do your SRA annually, if you haven't yet for 2022, now is the time.

**FOLLOW US ON LINKEDIN FOR OUR MONTHLY HEALTHCARE BULLETIN
AND WATCH FOR QUARTERLY WEBINAR AND LUNCH & LEARN OPPORTUNITIES
@CORE-BANK | #HEALTHCAREBANKINGBULLETIN | COREBANK.COM/WEBINAR**

AUTHORED BY:

Taya Gordon, EMBA, CMPE, CMOM

LinkedIn: https://www.linkedin.com/in/tayagordon/
Twitter: https://twitter.com/tayamoheiser