5 Things to Know About HIPAA Security Risk Assessments

Yearly Deadline: December 31st

1 Security Risk Assessments (SRAs) safeguard Protected Health Information (PHI)

The HIPAA Security Rule mandates that healthcare providers have adequate safeguards in place to protect PHI. Healthcare organizations are required to assess their physical, administrative, and technical safeguards annually to ensure that they are properly handling PHI. This is done through a security risk assessment. Conducting a security risk assessment identifies gaps in security practices; organizations must create remediation plans determining how they plan, or are already working, to close those identified gaps.

2 HIPAA Regulations Do Not Specify How to Complete an SRA

The Health Insurance Portability and Accountability Act (HIPAA) established industry standards for healthcare organizations. The law was meant to apply to all healthcare organizations, from single doctor practices to large hospital groups. As such HIPAA law is vague, allowing healthcare organizations to determine what they need to implement to adequately safeguard PHI. Although the Office for Civil Rights (OCR) provides some guidelines, they do not explicitly tell organizations what needs to be included in a security risk assessment. Organizations must determine what is right for them when assessing if they are correctly securing PHI.

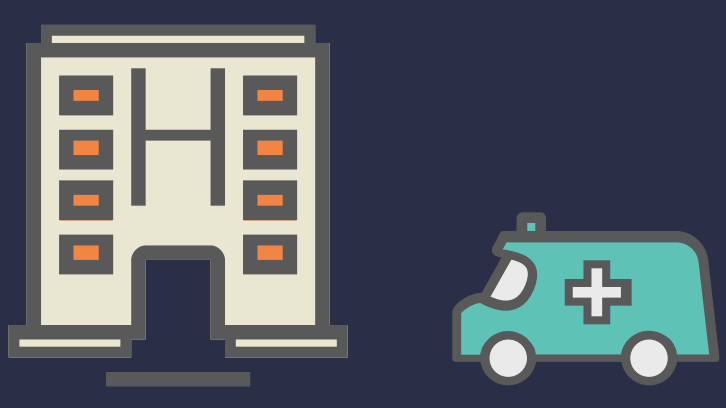
3 Lack of an SRA Can Result in Large HIPAA Fines

HIPAA fines are skyrocketing, with the average fine at $1.5 million. HIPAA violations, in many cases, are the result of human error. Losing a device or opening a malicious email link, can lead to HIPAA violations. A security risk assessment ensures that in the event of a breach, organizations will have the proper measures in place protecting PHI. HIPAA fines are not issued due to the breach itself, the OCR realizes that breaches are inevitable, fines are issued for lack of adequate safeguards. Conducting a security risk assessment allows healthcare organizations to identify where their security practices may be lacking, so that they can make necessary updates, minimizing their risk of HIPAA fines.

4 "Safe Harbor" Method

As stated previously, HIPAA fines are not issued for lost devices, but from lack of safeguards. HIPAA's "Safe Harbor" method gives healthcare organization guidelines that they should implement to de-identify patient information. De-identified information cannot be linked to a specific individual. De-identifying patient information protects healthcare organizations from HIPAA fines; if a device holding PHI is lost or stolen, PHI will be unreadable, making it likely that the organization will not be subject to fines.

5 SRAs Increase Cybersecurity



Cybersecurity should be a top priority for healthcare organizations. Conducting a security risk assessment allows organizations to identify areas in which their security is lacking so that they may address vulnerabilities.