MEDCURITY

Security Risk Analysis Checklist

What is a Security Risk Analysis?

The Health Insurance Portability and Accountability Act (HIPAA) requires covered entities and business associates to conduct a regular Security Risk Analysis to determine your organization's vulnerabilities to the security of Protected Health Information (PHI). In your SRA, you are required to:

Find where all PHI is stored, received maintained and/or transmitted

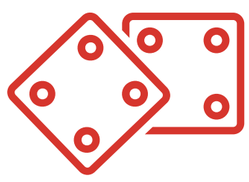
Whether the PHI is cloud-hosted, on a thumb drive or it's transmitted through a text or email, it must all be documented

Identify potential threats to your PHI

Try to identify particular threats that would affect your specific environment

Assess Current Security Precautions

Document the current safeguards your organization is implementing to secure PHI



Calculate the Likelihood of Threats Occurring

Determine the likelihood of all potential security risks to PHI

Determine the Impact if a Threat Occurred to PHI

For every potential threat, determine the severity of the affect if it were to occur

Document Findings and Create a Remediation Plan

Ensure this analysis is thoroughly documented, including links to your relevant policies and evidence. Create a plan to remediate risks related to your SRA

Periodically review and update SRA when necessary

Update your SRA anytime there are environmental changes within your organization. Complete an audit-ready SRA report annually by the December 31st deadline

Feeling overwhelmed? Check out medcurity.com to see how we can help you complete your SRA!