HIPAA Security Risk Assessment

This example assessment has been compiled by extracting controls from several recognized security frameworks. The controls included listed below represent the minimum required for an effective HIPAA security risk assessment, and it may be necessary for some organizations to add further controls in order to safeguard the confidentiality, integrity, and availability of ePHI.

To use this HIPAA security risk assessment, simply check the boxes when you have completed the control and review any unchecked boxes thereafter to see if the control applies to your organization. Remember to document the assessment, any actions you have taken to remediate security gaps, and any training you have provided to members of the workforce as a result of this assessment.

Physical Device Security Risk Assessment

□ Have you made an inventory of all physical devices within the organization that create, receive, maintain, or transmit ePHI?

□ Have you implemented measures to comply with all physical safeguards of the Security Rule (45 CFR §164.310)?

□ Have you made an inventory of all physical devices with remote access to ePHI including end users' personal devices (if applicable)?

□ Have you tested physical devices and systems for vulnerabilities that could permit unauthorized access, modification, or deletion of ePHI?

Access & Remote Access Security Risk Assessment

Have you implemented policies and procedures to comply with the following Security Rule standards applicable to remote access:

□ 45 CFR §164.308(a)(3) - Workforce security, including termination procedures?

□ 45 CFR §164.308(a)(4) - Information access management, including access authorization?

□ 45 CFR §164.308(a)(5) - Security awareness training, including password management?

□ 45 CFR §164.308(a)(6) – Security incident procedures, including incident reporting?

□ 45 CFR §164.312(a) – Access controls, including emergency access and automatic logoff?

□ 45 CFR §164.312(b) – Audit controls, including login monitoring and activity logs?

□ 45 CFR §164.312(c) – Integrity controls (Note: also applies to transmission security)?

□ 45 CFR §164.312(d) – Authentication controls, including MFA if reasonable and appropriate?

□ 45 CFR §164.312(e) – Transmission security, including the encryption of ePHI in transit?

Software & User Security Risk Assessment

□ Have you made an inventory of all software platforms and apps used in the organization to create, receive, maintain, and transmit ePHI?

Have all platforms and apps been subjected to:

□ Penetration testing?

□ Brute force password attacks?

Have all members of the workforce been tested on:

□ Their susceptibility to phishing emails?

□ Their susceptibility to phishing emails?

Threat & Threat Remediation Assessment

□ Have you determined the likelihood of all reasonably anticipated threats?

□ Have you determined the impact of each reasonably anticipated threat?

□ Are your existing security measures sufficient to reduce the impact of each reasonably anticipated threat to an acceptable level?

□ Are your existing security measures sufficient to reduce the impact of each reasonably anticipated threat to an acceptable level?

□ If not, have you prioritized vulnerabilities and threats according to their level of criticality?

□ Have you identified mechanisms, policies, and/or procedures to address identified vulnerabilities and threats?

□ Have these measures been discussed with appropriate members of the workforce to ensure they are workable and align with existing, non-security priorities?