HIPAA Risk Assessment Tip Sheet

General Requirements Risk Assessment

□ Do all members of the workforce understand what Protected Health Information is and why it must be protected?

□ Are all members of the workforce with access to PHI trained on the organization's HIPAA policies and procedures?

□ Do all members of the workforce participate in a security awareness program regardless of their access to PHI?

□ Does your security awareness program test users’ susceptibility to phishing and other social engineering techniques?

□ Does your organization provide a secure channel for members of the workforce to report HIPAA violations anonymously?

Part 162 Risk Assessment

□ Do you have procedures in place to ensure the correct NPI is used in eligibility, authorization, and other Part 162 transactions?

□ Do you have procedures in place to monitor changes to transaction code systems such as HCPCS and the National Drug Code?

Business Associate Risk Assessment

□ Have you identified all your business partners and software vendors that qualify as business associates as defined by §160.103?

□ Have you executed Business Associate Agreements with business partners and software vendors that qualify as business associates?

□ Do you monitor business associate compliance and factor any identified vulnerabilities or threats into your risk assessments?

Privacy Rule Risk Assessment

□ Does your Notice of Privacy Practices clearly explain permissible uses and disclosures of PHI to patients or plan members?

□ Is your workforce trained on which disclosures of PHI are permissible and which are subject to the minimum necessary standard?

□ Do you have documented procedures in place for complying with an individual's right to restrict disclosures of PHI?

□ Do you have documented procedures in place for responding to a right of access request from a patient or plan member?

□ Have you distributed a sanctions policy outlining the sanctions for non-compliance with the organization´s HIPAA policies?

Physical Security Risk Assessment

□ Have you got an inventory of all information systems and physical devices that create, receive, maintain, or transmit ePHI?

□ Have you implemented physical controls so that only personnel with authorization can access facilities, systems, and devices?

□ Have you implemented a facility security plan to safeguard the facility from unauthorized access, tampering, and theft?

□ Have you implemented and tested a data backup plan, an emergency mode operation plan, and a disaster recovery plan?

□ Do you have procedures to ensure the effective sanitization of devices and media before they are re-used or disposed of?

Technical Security Risk Assessment

□ Have you issued all members of the workforce with unique user IDs and instructed them not to share or disclose IDs?

□ Have you activated automatic logoff on all devices with access to ePHI including personal devices with remote access to ePHI?

□ Have you deployed solutions or configured systems to monitor user activity and ensure the integrity of ePHI at rest and in transit?

□ Is all ePHI at rest and in transit encrypted to render it unusable, unreadable, or indecipherable to unauthorized individuals?

□ Do you have procedures for accessing ePHI in an emergency? Are members of the workforce trained in activating the procedures?

Administrative & Breach Notification Risk Assessment

□ Have you assigned security roles and responsibilities to all members of the workforce with access to PHI?

□ Do you have procedures in place to quickly retrieve documentation if, for example, it is requested by HHS' Office for Civil Rights?

□ Do you have procedures in place for receiving reports of data breaches from downstream business associates?

□ Can you satisfy the burden of proof standard (§164.414) that all notifications required by the Breach Notification Rule are made?

□ Have you scheduled a review of this assessment after any new policies, procedures, or security measures have been implemented?