HIPAA Security Risk Assessment Template

How to Use this Template

This template provides the basic information a HIPAA covered entity or business associate should include in a HIPAA security risk assessment. You are invited to use it “as it”, customize it to your specific requirements, or integrate it into an existing HIPAA security risk assessment.

To use the template, tick off each box as you complete each step of the assessment. If you are unable to tick off any box, highlight it for attention. Then prioritize the highlighted boxes to address the threats and vulnerabilities considered to have the greatest potential impact.

Physical Security Risk Assessment

□ Make a list of all information systems and physical devices that create, receive, maintain, or transmit ePHI?

□ Implement procedures and physical controls so that only personnel with authorization can access systems and devices.

□ Develop and implement a facility security plan to safeguard the facility from unauthorized access, tampering, and theft.

□ Develop and test a disaster recovery plan to include data backup/restoration and emergency mode operations.

□ Implement procedures to effectively sanitize devices and media of ePHI before they are re-used or disposed of.

Technical Security Risk Assessment

□ Issue all members of the workforce with unique user IDs and instruct them not to share or disclose IDs.

□ Activate automatic logoff on all devices with access to ePHI including personal devices with remote access to ePHI.

□ Implement solutions or configure systems to monitor user activity and ensure the integrity of ePHI at rest and in transit.

□ Encrypt all ePHI at rest and in transit so it rendered unusable, unreadable, or indecipherable to unauthorized individuals.

□ Develop procedures for accessing ePHI in an emergency and for activating the procedures. Train users on these procedures.

Administrative Security Risk Assessment

□ Assign security roles and responsibilities to all members of the workforce - not just the compliance and IT teams.

□ Maintain (and document) an ongoing security awareness program for all members of the workforce including management.

□ Apply sanctions fairly and equally for all policy violations - especially when violations are committed by management.

□ Develop and test a communication chain of command for reporting and responding to security incidents.

□ Schedule a review of the assessment for an appropriate time after any new security measures have been implemented.

General Security Risk Assessment

□ All business associates and subcontractors have been identified and the required Agreements are reviewed and up to date.

□ We maintain copies of business associates' and subcontractors' security policies to monitor compliance with HIPAA.

□ Data flows are mapped internally and with business associates or subcontractors.

□ We conduct penetration testing on all information systems, devices, software platforms, and apps.

□ We test our workforce's susceptibility to phishing and other social engineering techniques.