CHECKLIST

HIPAA Self-Assessment

LayerCompliance™ by CAEK

The following questionnaire is provided for self-assessment of your current HIPAA security compliance program. It is not intended to offer advice or recommendations for achieving compliance with the HIPAA Security Rule. This questionnaire is not intended as a Risk Analysis or assessment. For more information, visit www.LayerCompliance.com.

☐	Have you performed a Risk Analysis in the past year? Is your Risk Analysis a comprehensive report (not a checklist) that identifies all 64 HIPAA Security standards?
☐	Is your Risk Analysis a comprehensive report that specifically identifies the likelihood, impact, and risk score of common threats? (Examples include ransomware, lost or stolen devices, natural disasters, etc.)
☐	Do you have written documentation of your HIPAA activities to demonstrate that your policies have been implemented?
☐	Do you have a written Risk Management Plan, including documentation of ongoing HIPAA activities?
☐	Do you have a written policy for hiring employees that includes providing access to protected health information (PHI) according to their job role?
☐	Do you have ***written*** documentation that all account access has been disabled or passwords changed for all employees who have been terminated in the last year?
☐	Do you have documentation that all computers (servers, desktops, laptops, mobile devices) that contain PHI are encrypted?
☐	Do you have a signed Business Associates Agreement as revised by the 2013 HIPAA Omnibus Rule for all vendors who may access, store, or transmit PHI? (Examples include IT vendors, third-party marketing vendors, business managers, 3rd party applications that connect to your practice management system, etc.)