HIPAA Risk Assessment

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that you perform a periodic "risk assessment" of your practice. A risk assessment is a mandatory analysis of your practice that identifies the strengths and weaknesses of the safeguards your practice has in place to protect patient information and privacy. A risk assessment should include an evaluation of at least three types of safeguards you should use in your practice: (1) physical safeguards; (2) technical safeguards; and (3) administrative safeguards.

A risk assessment is a formal process and must be documented in writing. The risk assessment should include documented review of each type of safeguard, as well as any identified weaknesses and/or deficiencies of those safeguards in your practice. After you identify any existing weaknesses and/or deficiencies in your safeguards, you should either take the appropriate steps to address those weaknesses and/or deficiencies in your safeguards or document the reasons why you cannot reasonably address or implement those safeguards.

Remember, each practice is unique and a risk assessment must consider these differences in privacy and security needs, resources, and capabilities. For example, a risk assessment for a specialty surgical group comprised of 20 physicians may look very different from a risk assessment for a medical practice with two or three psychiatrists.