Health Information Compliance Alert

Reader Question: Don't Be Fooled By 'HIPAA Certification' Schemes

Question: We recently got a flier from a compliance company touting that it could certify our practice as compliant with the HIPAA Security Rule after a review of our policies and procedures for a flat fee. Is there even such a thing as a HIPAA certification for a medical practice?

Texas Subscriber

Answer: No, HIPAA certification is not a thing, and vendors marketing that they can certify your policies after looking at your systems and data are not to be trusted. In fact, "there is no standard or implementation specification that requires a covered entity to 'certify' compliance" at all, according to HHS Office for Civil Rights (OCR) guidance.

However, the HIPAA Security Rule does require covered entities (CEs) to annually evaluate policies and procedures, assess risks, and manage the issues through updates. These compliance check-ups can be done by your IT staff or outsourced to a compliance expert, but there is no certification process or credential for being HIPAA compliant.

"It is important to note that HHS does not endorse or otherwise recognize private organizations' certifications' regarding the Security Rule, and such certifications do not absolve covered entities of their legal obligations under the Security Rule," warns OCR guidance. "Moreover, performance of a 'certification' by an external organization does not preclude HHS from subsequently finding a security violation."