NIST Seeks Comments on Version 2.0 of HIPAA Security Rule Compliance Guidance

“Cyber threats and cybersecurity controls have evolved significantly over the past two decades since the HIPAA Security Rule were originally promulgated. During this same time, healthcare entities have increasingly become a prime target of hackers seeking to extort payment using ransomware, exfiltrate patient data to commit fraud, or disrupt operations in other nefarious ways,” write Alaap B. Shah and Patricia M. Wagner in ***The National Law Review***.

“Recognizing these challenges, some security professionals have sought further clarity on the HIPAA Security Rule that they deem to be ‘long in the tooth’. Yet, regulators have not made any significant modifications – perhaps driven by the original policy considerations of the HIPAA Security Rule that: ‘the standard should be comprehensive and coordinated to address all aspects of security’; that it be “scalable, so that it can be effectively implemented by covered entities of all types and sizes’; and that it ‘not be linked to specific technologies, allowing covered entities to make use of future technology advancements.’

Read the article.