NEWS

Alisa Chestler Talks with *Wolters Kluwer Health Law Daily* About Patient Data Security

Data breaches can be nightmares for covered entities (CEs) and business associates (BAs) in terms of bad publicity, costs required to repair the breaches, and penalties imposed by HHS. The Health Insurance Portability and Accountability Act (HIPAA) Security Rule outlines administrative, physical, and technical safeguards that CEs and BAs must implement to keep electronic protected health information (ePHI) secure. A key technical safeguard is the encryption of ePHI. Despite the applicable regulations, breaches resulting from unencrypted ePHI continue to occur. Alisa Chestler recently spoke with Wolters Kluwer *Health Law Daily* about encryption guidelines, the encryption process, why breaches related to unencrypted data still occur, and how far CEs and BAs should go to encrypt ePHI.

Ms. Chestler noted that it is "nearly impossible" to create a plan based on a security risk analysis that says it will do anything other than encrypt data at motion—data being transmitted, data at rest—data being stored, and data in use. It may be possible, however, in instances of incidental use. If a CE or BA has a policy against using email to transmit PHI, it could be reasonable for the entity not to purchase an encryption and an emergency email may not be acceptable.