Report on Patient Privacy Volume 18, Number 4. April 30, 2018
OCR Offers Tips for Effective Contingency Plans

By HCCA Staff

"Don't wait for a disaster to happen before designing and implementing a contingency plan."

That's the concluding sentence in the March newsletter issued by the HHS Office for Civil Rights (OCR), which provides monthly advice and information to HIPAA covered entities (CEs).

As the newsletter points out, having contingency plans "aren't just a good idea," but the security rule requires both CEs and business associates (BAs) to "establish and implement" them.

Because organizations are often consumed with daily HIPAA compliance tasks, this requirement doesn't always get the attention it needs. But contingency plans are becoming even more important as ransomware attacks grow (see story, p. 1). Affected CEs and BAs can survive such attacks—without paying a ransom—if they have adequate backup systems and can maintain access to patient records, devices and other functions that are tied to electronic networks that have become compromised.