Report on Medicare Compliance Volume 28, Number 34. September 30, 2019

State Lawmakers Focus on Breach Notification, Credit Monitoring

By Jane Anderson

Multiple states continue to tighten their data privacy and breach notification laws, as new laws in states from New York to Texas take effect.

With the passage last year of breach notification legislation in Alabama and South Dakota, all 50 states now have these laws on the books. States are moving to shorten notification periods, require long-term credit monitoring and, in some cases, expand the definition of what's considered "personal information" in a breach.

In one of the biggest state legislative data security and privacy efforts in 2019, New York lawmakers approved the Stop Hacks and Improve Electronic Data Security (SHIELD) Act and the Identity Theft Prevention and Mitigation Services Act. Both bills were signed July 25 by Gov. Andrew Cuomo (D); the SHIELD Act takes effect next March, while the identity theft legislation takes effect in September.

The SHIELD Act expands the definition of private information to include Social Security numbers, financial account numbers, passwords or security codes, biometric data, and a username or email address in combination with a password or security question and answer. The new law does not include health insurance identifiers, however.

The act also broadens the circumstances that qualify as a breach and requires notification for any breach that includes New York residents' personal information, regardless of whether the entity conducts business in New York. Finally, it requires entities to implement reasonable safeguards to protect personal information; businesses in compliance with HIPAA are considered to be in compliance with this requirement.