COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 22, Number 12. December 07, 2022 Not Just OCR: States Increasing Focus On Security, 'Sensitive' Data Protections

By Theresa Defino

The HHS Office for Civil Rights (OCR) was satisfied enough with corrective actions implemented by a home health provider following an email phishing attack two years ago that it took no enforcement action.

But when it came to Massachusetts officials, Aveanna Healthcare—based in Georgia—wasn't off the hook. In just one recent example of state sanctions for privacy or security violations, Aveanna agreed to pay $425,000 for alleged violations of commonwealth law.[1] In this case, just 4,000 or so Massachusetts residents were among the 166,077 whose protected health information (PHI) was exposed.

In addition to exercising authority to bring action for HIPAA violations, states are increasingly flexing their (sometimes) collective muscle to pursue violations of consumer privacy laws, especially given there is no such federal law.

Raising the stakes further, state legislators are turning their attention to the issue of "sensitive" data—a concept that's evolving and varies among the five states that have new legislation in this area. Privacy and security officials need to keep up to date on state enforcement actions, laws and possible regulations, as well as the ramifications of class-action suits.