CARLTON FIELDS

Is Your Company Ready to Comply with Encryption of Individually Identifiable Health Information?

March 25, 2015

New Jersey's new data privacy standard, signed into law as S. 562 by Gov. Chris Christie on January 9, requires health insurance carriers that are authorized to issue health benefit plans in New Jersey to protect individually identifiable health information through encryption or "by any other method or technology rendering the information unreadable, undecipherable, or otherwise unusable by an unauthorized person." In addition to all other penalties provided by law, violating the statute shall mean a fine of not more than $10,000 for the first violation, and not more than $20,000 for all subsequent violations. This law was passed in the wake of a series of data breach incidents involving stolen laptops containing the unencrypted health information of nearly one million New Jersey residents. New Jersey's encryption requirement, which becomes effective on August 1, 2015, is more stringent than the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which requires health plans, health insurance carriers, and business associates (among others) to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic protected health information, and implement encryption of such information whenever deemed appropriate. Notwithstanding, encryption of electronic protected health information is already the standard for many HIPAA covered entities and business associates. Therefore, the encryption requirements imposed by this New Jersey statute may not result in practical changes for all that many health insurance carriers issuing plans in New Jersey. Of note, this New Jersey law, like many other data privacy laws with encryption provisions, does not address the fact that: (a) some entities employ encryption solutions that use simple algorithms and/or have other issues that make the data susceptible to unauthorized access; and (b) rendering the information "unreadable, undecipherable, or otherwise unusable" is an impossible goal because even the best encryption in the world can only make it extremely difficult to do these things – no one has ever made it impossible. Privacy law practitioners now group New

Jersey, Massachusetts, and Nevada together as states with information security requirements that are more rigorous than those imposed by federal or other states' laws.

Related Practices

Intellectual Property
Cybersecurity and Privacy
Technology
Health Care

Related Industries

Technology
Health Care