PUBLICATION

A New York State of Mind: The SHIELD Act

Authors: Layna S. Cook Rush
September 13, 2019

The Stop Hacks and Improve Electronic Data Security (SHIELD) Act, signed by Governor Cuomo on July 25, 2019, amends New York's data breach notification law for computerized data. The Act's new requirements take effect March 21, 2020.

The SHIELD Act's amendments subject businesses that *own or lease* the "Private Information" of New York residents to data security requirements, *regardless* of whether the business conducts business in the state of New York. The Act also expands the definition of "Private Information" to include biometrics (such as fingerprints, voice print, retina or iris images, or other unique physical representation used to authenticate an individual's identity) and email addresses or online usernames that are combined with a password or security question and answer that would allow access to online accounts.

The amendment expands the definition of a "Breach of the Security System" to include not only the acquisition of Private Information but also the mere access to Private Information. This change means that a business *may* have a notifiable data breach even if Private Information was only viewed and not printed or otherwise removed from the business's systems. In determining whether notification is required under the law, a business should conduct a risk of harm analysis to decide whether the type of Private Information that was accessed or acquired was of the type that might be misused, cause financial harm to the affected person, or cause emotional harm in the case of online credentials. If a business determines no notification is required, it must document the determination. Documentation should be maintained for five years. Additionally, if 500 or more New York residents are affected, a copy of the determination must be provided to the Attorney General within ten days of the determination.

The Act clarifies that if a business is regulated by the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), 23 NYCRR 500 or other laws that require notification, then the business is not required to give additional notice to affected individuals under the SHIELD Act. However, the business is still required to notify the Attorney General, the Department of State, the Division of State Police and consumer reporting agencies. The Act also requires HIPAA Covered Entities that report a breach to the Department of Health and Human Services (HHS) to provide notice to the Attorney General within five days of notifying HHS – even if the breach does not involve "Private Information" or is not computerized data. Failure to report may result in civil monetary penalties under the New York law.

The SHIELD Act also requires businesses that own or license computerized data – which includes Private Information of a resident of New York and that is otherwise subject to, and in compliance with, certain data security laws – to develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the Private Information, including, but not limited to, disposal of data. The Act defines how to determine whether a business is "in compliance" for purposes of this standard, and includes things such as having a designated employee to coordinate the security program, performing reasonable identification of foreseeable internal and external risks, training employees and ensuring service providers have reasonable security safeguards, etc.

While there is still no private right of action in the law, failure to comply with the SHIELD Act can result in civil monetary penalties in a claim brought by the Attorney General.

In conjunction with the new law, on August 12, 2019, the New York State Department of Health's Chief Health Information Officer for the Office of Health Information Management published new notification protocols for health care providers following a potential cybersecurity incident. The letter requires health care providers, including hospitals, nursing homes, diagnostic and treatment centers, adult care facilities, home health agencies, hospices and licensed homecare services agencies to report any potential cybersecurity incident to the Department.

While there is no timing requirement outlined in the letter, the Department makes it clear that this reporting is *in addition to* any other required reporting to agencies such as the New York Patient Occurrence Reporting and Tracking Systems, the State Attorney General, Department of State Division of Consumer Protection, Division of State Police, and any federal reporting requirements under HIPAA. The Department intends to use this notification to collaborate with partner agencies and aid providers who are experiencing cyber events.

The Takeaway?

If you do business with New York residents, you should ensure you are compliant with the new SHIELD Act amendments. Furthermore, if you are a health care provider, update your cyber response plan to comply with the notification protocols published by the Department of Health.

If you have any questions regarding these issues or any other data privacy or security breach related issues, please contact Layna Cook Rush or any of the attorneys in Baker Donelson's Data Protection, Privacy and Cybersecurity Group.