Published on *The National Law Review* https://natlawreview.com

SHIELD Act Becomes Law, Expanding Breach Notification and Data Security Requirements

Article By:

Leslie J. Levinson

On July 25, 2019, New York Governor Andrew Cuomo signed the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) into law. The SHIELD Act modifies the current Breach Notification Law to expand the types of data elements that are considered "private information" and to expand the data breach disclosure requirements for individuals and businesses. Moreover, the law creates a requirement that owners or licensors of private information meet a new "reasonable security requirement."

Breach Disclosure

The SHIELD Act updates the breach notification requirements so that they apply to all individuals or businesses who own or license private information of a New York resident, not just to those that "conduct business" in New York State and expands the current law's definitions of "private information" and "breach." These changes have far reaching implications to persons or businesses who own or license private information of New Yorkers and significantly lowers the threshold of what is considered a breach that triggers a disclosure to affected persons.

Previously, "private information" referred to a combination of personally identifying information paired with a social security number, or driver's license number, or credit card number along with its security code. The SHIELD Act keeps the same combination but also considers personal identifiers in tandem with credit card numbers without security codes, and biometric data—electronic measurements of physical characteristics such as a finger print, voice print, or retina or iris image—to be "private information." Furthermore, under the new law, "private information" also means "a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account." Additionally, the law expands the definition of a "breach." Previously, a breach occurred when private data was *acquired* by an unauthorized individual. Under the new law any time private data is *accessed or acquired* without authorization there is a breach.

Notices of a breach sent by health care entities to affected persons that are consistent with the requirements of the "regulations implementing the Health Insurance Portability and Accountability Act of 1996 [(HIPAA)] (45 C.F.R. parts 160 and 164), … and the Health Information Technology for Economic and Clinical Health Act [(HITECH)]" are sufficient under the SHIELD Act. However, the law does require those covered entities to provide notification to the New York Attorney General's Office

within five (5) business days of notifying the Secretary of Health and Human Services.

Reasonable Security Requirements

Under the SHIELD Act, there are also new reasonable security requirements that every owner or licensor of private information must meet. Compliance requires the implementation of reasonable administrative, technological, and physical safeguards on all private information.

A New York health care entity in compliance with the security requirements for HIPAA and HITECH is considered a “compliant regulated entity,” which will be deemed in compliance with the new statutory reasonable security requirements.

In light of the unique compliance methods offered by the SHIELD Act for health care entities already regulated by HIPAA and HITECH, health care entities should ensure their data security programs are in compliance with HIPAA and HITECH and also be vigilant of data breaches outside their scope which may also require disclosure under the SHIELD Act.

This post was co-authored by Michael Lisitano, legal intern at Robinson+Cole. Michael is not yet admitted to practice law.

National Law Review, Volume IX, Number 214