**New York's Shield Act: What it Means for Podiatrists**

**By:  Matthew S. Feldman, Esq., General Counsel**

**New York State Podiatric Medical Association**

New York recently enacted the Stop Hacks and Improve Electronic Data Security (SHIELD) Act in response to growing concerns about data security. The SHIELD Act amends the New York General Business Law to provide broader safeguards for consumer data by (1) expanding territorial application of data security protections; (2) encompassing more types of data; (3) expanding the definition of "breach"; and (4) effective March 21, 2020, imposing new data security requirements on businesses and employers.

The SHIELD Act broadens the scope of the previous protections in several ways. First, the Act applies not only to personally identifiable information but also to "private information", which is personal information in combination with any one or more of the following data elements: (1) social security number; (2) driver's license/non-driver ID; (3) account number; (4) credit/debit card number with security code/access code/password or other information that would permit access to the account; a username or email address in combination with a password or security question and answer that would permit access to an online account; and/or any unsecured health information held by a covered entity as defined by HIPAA. Second, while the previous protections applied only to businesses located in New York, the SHIELD Act applies to any person or business that owns or licenses computerized data that includes the private information of New York residents, regardless of the physical location of the person or business. In addition, the Act significantly expands the definition of what constitutes a breach requiring notice to affected persons. While previously a breach required "acquisition" of data, the Act requires only "unauthorized access."

Beginning on March 21, 2020, all persons and businesses covered by the SHIELD Act are required to develop, implement, and maintain "reasonable safeguards" to protect the integrity of private information. The Act does not explicitly define what constitutes sufficient "reasonable safeguards," however it does provide a non-exhaustive list of examples including administrative safeguards such as designating one or more employees to coordinate the security program, security training for employees, selecting service providers capable of maintaining appropriate safeguards, and adjusting security programs in light of new business and/or circumstances; technical safeguards such as risk assessment in network, software design, and information processing; as well as regular monitoring and testing of the system; and physical safeguards such as risk assessment of information storage and disposal; detecting, preventing, and responding to intrusions; and disposing of private information after a reasonable amount of time after it is no longer needed for business purposes. Healthcare providers benefit from the fact that data storage policies and practices that comply with existing privacy regulations, including HIPAA, are considered to be compliant with the SHIELD Act's reasonable safeguards requirement. It is important for healthcare practitioners and entities to regularly assess and evaluate their data security policies in order to ensure compliance with both HIPAA and the SHIELD Act and many IT professionals offer these services to their clients.

In the event of a breach of personal or private information, businesses are required to provide notice to affected consumers "in the most expedient time possible," and without unreasonable delay. If the breach involves more than 500 consumers, notice must also be given to the Attorney General, Department of State, and State Police. There are exceptions to the breach notification requirement: In the case of an inadvertent disclosure by a person authorized to access private information, the breach does not have to be reported so long as a reasonable determination is made that the exposure will not result in misuse or harm to the person whose information was affected. The determination must be documented and retained for five years. Also, if notice of the breach of the security of the system is made to affected persons pursuant to another state or federal privacy protection, including HIPAA, additional notice to those persons is not required under the SHIELD Act. Noncompliance with the SHIELD Act can result in substantial civil penalties and may be investigated by the Attorney General. Although there is no private right of action, the Attorney General may initiate an action to enjoin further violation. Violators may also incur civil penalties of the greater of $5000 or up to $20 per violation, with a maximum penalty of $250,000. Actions can be brought up to six years following the noncompliance.

The SHIELD Act addresses mounting consumer privacy concerns by providing broad protections to consumer information and imposing heightened compliance requirements on persons businesses who retain the personal and/or private information of New York residents. Although all types of New York businesses and employers are affected by the new requirements, compliance is especially important in the healthcare industry due to the degree of private information maintained. To ensure compliance, practitioners and/or entities should review their existing policies to make sure they have adequate protections in place.