NPIP

Risk Alert
August 2019

Data Breach Legislation Update

Legislation regarding the definition of personal information and the revision of data breach notifications was recently passed into law as part of House Bill 1071. The amendments will take effect on March 1, 2020.

What is the new definition of personal information?

Previous definition of personal information	*Expanded definition going into effect March 1, 2020*	*Additional items included in the expanded definition*
A person's name in combination of any of the following: • Social security number; • State identification card number; or • Financial account or credit card number, in combination with any ○ Required security code; ○ Access code; or ○ Password that would permit access to an individual's financial account	A person's name in combination of any of the following: • The previous definition • Full date of birth; • Private, unique keys used to authenticate electronic records; • Student, military, or passport identification number; • Health insurance policy or identification number; • Information about medical history or mental or physical condition, or medical diagnosis or treatment; or • Biometric data of an individual's biological characteristics such as fingerprints, voiceprints, eye retinas, irises, or other unique individual biological patterns or characteristics	• Any of the previously listed information **without** the consumer's name if: ○ The data is not encrypted or redacted; or ○ If the data would lead a person to commit identity theft • Usernames or email addresses in combination with a password or security questions and answers that would allow access to an online account

How have data breach notification requirements changed?

The period of time to provide notice to parties affected by a data breach, as well as the attorney general has shortened to 30 days, and notices must include the following information:

- The types of personal information that are reasonably believed to have been the subject of the breach
- Timeframe of exposure, including the date of the breach and the date of the discovery of the breach
- Summary of the steps taken to contain the breach

What does this mean for my organization?

Implementing and adhering to a data retention or destruction plan can help prevent your organization from storing unnecessary personal information. We strongly recommend that you review and/or update your data retention plans to reduce or eliminate any of the information listed above from your records. Associated expenses related to a data breach – notifications, credit monitoring services, etc. – can quickly become exponential depending on the number of people affected, which can quickly exhaust insurance limits. You can greatly reduce your organization's exposure by only maintaining required information and making sure it is secured and disposed of properly.

Administered By:

CLEAR risk solutions

Questions? Please contact your local broker or your Clear Risk Solutions risk manager directly at 800.407.2027