SQUIRE PATTON BOGGS

Insurance Data Security Model Law

The NAIC's Cybersecurity Task Force released a new draft model Insurance Data Security Law in August and is requesting comments by Friday, September 16, 2016. The draft addresses the many comments received after the task force released its first draft back in April. The new draft consolidates sections, simplifies references to other relevant state law and redefines its scope and effect.

In Section 2, Purpose and Intent, the new draft makes it clear that this law establishes the exclusive standards in the enacting state for data security and investigation and notification of a data breach affecting an insurance licensee or its third-party service provider. It is mainly a consumer statute focusing on the unauthorized acquisition, release or use of an individual's personal information.

Section 3 includes definitions. The definition of licensee was modified in this draft to include "any person or entity licensed, authorized to operate, or registered, or required to be licensed, or registered pursuant to the insurance laws of this state." Note that the definition no longer uses words like "insurers" or "producers," but focuses on the license or registration under that state's insurance laws.

Personal information is also defined in four subsections to include financial account numbers, a consumer's name in combination with ten other data elements (including non-truncated social security number, date of birth and biometric data), certain data elements identified that even when not in connection with the consumer's name would be sufficient to permit identity fraud and health care information.

In Section 4, the model law describes the information security program that every licensee must develop. Notably, the elements of the program are linked to the size and complexity of the licensee, the nature of the licensee's activities and the sensitivity of the personal information in the licensee's possession or control. In other words, there are minimal requirements and prudential standards, but no exact formula that each licensee must follow. This allows for smaller entities and entities with less risk to have a less rigorous and costly program. Nevertheless, every licensee must document on an ongoing basis compliance with its information security program.

Section 4D sets out the minimum requirements for a licensee's information security program. It requires the program to be designed to mitigate identified risks based on generally accepted cybersecurity principles. Notably, this draft eliminates reference to the National Institute of Standards and Technology Cybersecurity Framework in favor of a more generic statement.

Among the security measures that should be included in each licensee's program, as appropriate, are authentication controls, restricted access, encryption, state of the art authentication procedures, regular testing, response procedures, procedures to protect against destruction of personal information by hazards and procedures for secure disposal of information. Board of directors oversight and oversight of third-party service provider arrangements is required.

Section 5 describes the investigation process should there be a data breach. Minimum requirements are established, including assessing the nature and scope of the data breach or potential data breach, identifying personal information possibly involved, determining whether personal information has been acquired or released and restoration measures. Section 6 describes the notification requirements. This section dovetails with each state's notification laws, but requires that the insurance regulator be noticed along with other relevant government entities. The insurance regulator has the right to review a licensee's draft written communication to consumers to ensure compliance with the statute.

Other sections cover notice when third-party service providers have a breach, consumer protections following a breach, the power of the insurance regulator to investigate and examine any licensee concerning compliance with this law and enforcement proceedings. The enforcement proceedings dovetail with each state's insurance laws or administrative procedures act.

After receiving comments, the NAIC's Cybersecurity Task Force will either come out with another draft or advance the model law to the NAIC for promulgation. If you need assistance in evaluating the draft and providing comments to the NAIC, please let us know and we will be happy to help.

Contacts

Larry P. Schiffer
Partner
T +1 646 557 5194
E larry.schiffer@squirepb.com