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

Insurance Regulators Fine Tuning Cybersecurity Guidance

Article By:

Privacy & Security Practice Group at Mintz Levin

You may not realize how much personal information your insurance company has about you. Scarier still is that much of this data is sensitive and valuable to hackers – such as your Social Security number, financial information, medical history, even itemized schedules of your most expensive personal property. As data breaches affecting insurers have piled up in the past couple of years (Anthem, Premera Blue Cross and Blue Shield, Excellus Health Plan, UCLA Health System just to name a few), so too have calls for stronger data security protections applicable to insurance data. In response, the CyberSecurity Task Force of the National Association of Insurance Commissioners ("NAIC"), the standard-setting organization in the U.S. insurance industry created and governed by the chief insurance regulators from the 50 states, the District of Columbia, and five U.S. territories ("Task Force") is racing to finish its ***Insurance Data Security Model Law ("Model Law" or "Law")*** by the end of this year so that states can begin the adoption process as early as 2017.

Some helpful background. Before publishing the first draft of the Model Law in April of this year, the Task Force issued the Principles for Effective Cybersecurity: Insurance Regulatory Guidance centered on the protection of the insurance sector's infrastructure and data from cyber-attacks and the NAIC Roadmap outlining an insurance consumer "bill of rights". As currently drafted, the Model Law applies to "any person or entity licensed, authorized to operate, or registered, or required to be licensed, authorized or registered pursuant to the insurance laws of [the state where the Law is enacted]" (we'll refer to these persons or entities as "Insurers" in this article). After an outpouring of comments on the Model Law from industry, trade groups, and regulators, the Task Force recently published a revised draft. This comparison of the two drafts illustrates how the Task Force has tried to make the Model Law more clear, workable and palatable to stakeholders. We provide a high level overview of the key changes below.

What's changed? Here is a summary of the key differences between this latest draft of the Model Law and the April draft:

- Preemption. The revised Model Law appears to leave intact any existing federal or state law that does not conflict with the terms of the Model Law. In effect, this means that the Model Law may not supersede obligations that apply to certain Insurers under the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, and state statutes. If this loose preemption provision remains, the Model Law will likely fall far short of its stated goal to establish exclusive and consistent regulation for data security and standards applicable to the investigation and notification of data breaches in the insurance sector. In fact, it could very

well have the opposite effect and breed a new layer of regulation that exists alongside the existing patchwork of federal and state laws.

- No private right of action. The concept of a private right of action has been removed entirely. The Task Force likely moved in this direction in response to concerns from trade associations and industry commentators that such a provision would create uncertain litigation exposure and would not adequately empower consumers to pursue remedies in an efficient and cost-effective manner. However, the Model Law does not restrict a private right of action otherwise imposed by federal or state laws applicable to Insurers.

- Key Definitions. The revised draft reformulates the data breach definition with an encryption safe harbor, and defines "Personal Information" beyond an already broad scope of data so that it also picks up a consumer's date of birth and any information of the consumer that the Insurer has a legal or contractual duty to protect from unauthorized access or public disclosure. On the other hand, the "Consumer" definition has been somewhat narrowed to cover only individuals (and no longer entities) whose information is in the possession, custody or control of the Insurer.

- Information security program requirements. Insurers will be required to develop and maintain on an ongoing basis an information security program that is appropriate given the size of the Insurer and the nature and complexity of its business and that is based on "generally accepted cybersecurity principles" rather than on the National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*.

- Third Party Vendors. The obligation that Insurers include certain contractual requirements in their contracts with third party service providers (e.g., data breach notification requirements, indemnification, audit rights) has been deleted, but Insurers still have an obligation to contract only with third party providers capable of protecting personal information. Most importantly, the Insurer is now responsible for any failure by its third party vendors to protect personal information provided by the Insurer consistent with the Model Law.

- Heavy Notification Requirements. Insurers' notification requirements following a data breach are wide-ranging and no longer tied to a "substantial harm or inconvenience" trigger that would have permitted them to avoid notification requirements if they determined that a data breach was not reasonably likely to cause identity theft or fraudulent transactions on financial accounts. Under the revised draft, if an Insurer determines following an investigation required under the Section 5 of the Law that an unauthorized acquisition of certain personal information has occurred (this is the personal information listed under Section 3H(1), (2)(a) through (f), (3) or (4) of the Law), the Insurer must notify: consumers affected by a data breach, the insurance commissioner in their home state and in all states in which an affected consumer resides, law enforcement agencies, consumer reporting agencies if the breach affects more than 500 consumers, and any relevant payment card networks. The level of detail and guidance that must be included in the various notices is also far more extensive than what is required by most state data breach notification laws.

- Penalties. Specific monetary penalties have been abandoned and replaced with language to trigger an enacting state's general penalty statute for purposes of assessing violations.

The Model Law remains a work in progress. There remain some particularly problematic areas of

the Model Law that we encourage interested parties to closely examine. For example:

- Notification Timing. The revised draft requires an initial notification to insurance commissioners **within three business days of determining that a breach has occurred**. This timing requirement is simply not feasible given the time it takes to investigate a data breach, hire forensic consultants if appropriate, and coordinate with advisors and counsel to understand and digest the facts. Such a short window will force companies to provide incomplete and unreliable information to insurance commissioners that could prove misleading. Strangely, notification to consumers must be completed within 60 days of discovering a breach, which is far more lenient than what is permitted by most states' data breach notification laws.

- Lack of clarity. Several of the standards used in the revised draft will leave Insurers uncertain about what constitutes an adequate information security program and what types of security standards and measures should be adopted to achieve compliance with the Model Law.

What's next? The NAIC closed the written comment period on the revised draft of the Model Law on September 16th. Given the changes and issues outlined above, we expect that public comments to the current draft of the Law will generate further revisions and a last round of comments before the NAIC issues its final draft of the Law for adoption by the NAIC's Executive Committee. There will likely also be opportunities for public comment at the state level before the law is enacted in individual states. While adoption by individual states may be seem to be a little ways away, this is the time to begin thinking about what kind of changes you may need to make in your processes and procedures and to put in place an implementation plan to be compliant with the Model Law. We will continue to monitor developments with the Model Law and will keep you updated!

National Law Review, Volume VI, Number 299