Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Dissecting NAIC's Insurance Data Security Model Law

By **Lawrence Hamilton, Jeffrey Taft, Matthew Bisanz and Evan Sippel-Feldman**
November 28, 2017, 1:06 PM EST

Lawrence Hamilton

Jeff Taft

Matt Bisanz

Evan Sippel-Feldman

On Oct. 24, 2017, the National Association of Insurance Commissioners adopted an Insurance Data Security Model Law.[1] The Model Law builds on existing data privacy and consumer breach notification obligations by requiring insurance licensees to comply with detailed requirements regarding maintaining an information security program and responding to and giving notification of cybersecurity events.

The Model Law is similar in many respects to the cybersecurity regulation that was issued earlier this year by the New York State Department of Financial Services (NYDFS).[2] However, the Model Law pertains solely to insurance licensees, and because it is only a model law, it will only apply to licensees in any given state if it is enacted into law by that state. Moreover, each state will have the freedom to modify the wording of the Model Law as it sees fit.

This article (i) describes the relevant definitions and scope of the Model Law, (ii) highlights some of the Model Law's substantive requirements and (iii) discusses some key takeaways for the insurance industry. For simplicity, our analysis assumes that a state will adopt the Model Law substantially as written.

Definitions and Scope

Licensee

The Model Law applies to any person operating under or required to operate under a license or registration issued pursuant to a state's insurance laws. "licensees" include not only insurance companies, but also other types of business entities and individual professionals who are licensed under a state's insurance law (i.e., insurance agents and brokers). The Model Law expressly excludes from the definition of licensee (i) purchasing groups or risk retention groups that are chartered and licensed in another state and (ii) insurers that are only assuming business in the state as reinsurers and are domiciled in another state.

Nonpublic Information

"nonpublic information" is defined as any information that is not otherwise publicly available and that is (i) business-related information, the unauthorized disclosure or use of which would cause a material adverse impact on the licensee (e.g., trade secrets); (ii) information concerning an individual that could be combined with specified data elements to identify the individual (e.g., traditional personally identifiable information); or (iii) derived from an individual or health care provider and related to certain health care information (except for age and gender). Like the NYDFS cybersecurity regulation, the Model Law broadly defines nonpublic information to include business-related information rather than just customer information.

Cybersecurity Event

A "cybersecurity event" is defined as any act resulting in unauthorized access to (or disruption or misuse of) electronically stored information. However, the Model Law definition does not include unsuccessful attempts to access nonpublic information, and it does not include unauthorized acquisitions of encrypted nonpublic information unless the decoding key is also acquired. The Model Law also excludes from the definition of cybersecurity event situations where the licensee determines that the nonpublic information accessed by an unauthorized person was not used or released and has been returned or destroyed.

Third-Party Service Provider

A "third-party service provider" is defined as any person that is not a licensee, but contracts with a licensee to maintain, process, store (or otherwise has access to) nonpublic information.

Substantive Requirements

Tracking the NYDFS cybersecurity regulation, the Model Law requires every licensee (unless exempted) to maintain a written cybersecurity policy and to implement a risk-based cybersecurity program. A licensee must also satisfy specific requirements related to (i) maintaining an information security program, (ii) risk assessment and management, (iii) third-party service providers, (iv) incident reporting, investigation and notification, (v) annual certification and (vi) exemptions (if eligible).

Information Security Program and Board Oversight

The Model Law requires each licensee to maintain an information security program that is broadly designed to protect its nonpublic information. Additionally, the licensee's senior management must report to the licensee's board of directors at least annually on the overall status of the information security program, including the results of risk assessments, strengths or weaknesses of its current risk management controls, the outcome of any testing, third-party service provider arrangements and cybersecurity events. The required reporting must also detail any recommended changes to the information security program.

Risk Assessment and Management

Like the NYDFS regulation, the Model Law requires regular risk assessments to test the adequacy of the licensee's information security program (at least annually for key controls and systems). The licensee must designate either an internal team or an outside vendor to identify reasonably foreseeable risks that could lead to unauthorized access to nonpublic information.

Informed by the risk assessment, a licensee is expected to develop comprehensive written policies and procedures for cybersecurity. The Model Law anticipates that a licensee's cybersecurity policies and procedures will evolve based on emerging threats or vulnerabilities. Accordingly, the licensee is expected to provide recurring training to educate its personnel on their obligations to secure and protect nonpublic information.

Incident Reporting and Cybersecurity Event Notification

Every licensee also is required to prepare a written incident response plan to enable it to promptly respond to and recover from a cybersecurity event. The Model Law requires licensees to investigate and provide notice of a cybersecurity event to the following state insurance regulatory officials within 72 hours of determining such an event has occurred. First, a licensee must notify its home state regulator of any cybersecurity event if that state has adopted the Model Law. Secondly, a licensee must notify the insurance regulatory officials of a state other than its home state if the cybersecurity event involves the information of 250 or more consumers residing in that state and either (i) federal or state law requires the licensee to disclose the incident to a governmental body or (ii) the cybersecurity event has a reasonable likelihood of materially harming any consumer residing in the state or any material part of the normal operation of the licensee.

This notice obligation does not replace any obligation the licensee may have to provide consumers or state agencies with notice under a state's data breach notification law.

Annual Certification

Each insurer is required to submit an annual certification to the insurance regulator of its state of domicile, affirming its compliance with the information security program provisions of the Model Law. To the extent an insurer has identified areas that require improvement, updating or redesign, it must also document the remedial efforts that are underway or planned. In notable contrast to the NYDFS regulation, this annual certification requirement only applies to insurers and not to insurance producers.

Exemptions

Employees and agents of a licensee who are themselves licensees are not required to develop their own information security programs as long as they are covered by their organization's program. However, they remain subject to the other requirements of the Model Law, namely, the cybersecurity event investigation and notification requirements.

A licensee that has fewer than 10 employees, including independent contractors, is exempt from the information security program requirements of the Model Law. Further, a licensee subject to the Health Insurance Portability and Accountability Act (HIPAA) may simply certify its compliance with HIPAA's information security program requirements in order to satisfy the Model Law's information security program requirements.

The Model Law's exemptions are somewhat narrower than those provided under the NYDFS regulation in that the Model Law does not provide a partial exemption for licensees with less than $5 million in gross revenue in a state or less than $10 million in assets. Also, according to a drafting note in the Model Law, the intent of the drafters was that a licensee's compliance with the NYDFS cybersecurity regulation would also satisfy a licensee's obligations under the Model Law.

Some Key Takeaways for Insurance Industry

First, as noted above, the Model Law represents a significant effort by the NAIC to protect nonpublic information in the hands of licensees. However, because the Model Law is only an NAIC model, the actual adopted versions of the law may vary from state to state. Therefore, licensees need to carefully monitor when the Model Law is enacted into law in the states where they are licensed and whether the enacted version deviates from the text of the Model Law. Needless to say, significant deviations among the states could make compliance more difficult.

Second, while the Model Law generally follows the example of the NYDFS regulation, the text is more limited in scope and less prescriptive in its requirements. One of the benefits of a less prescriptive law is more flexibility for licensees. One downside is that each licensee will need to make its own judgments based upon its risk appetite with respect to their compliance with the law. This will likely raise interpretive questions as states adopt the Model Law or statutes based on it.

Third, the Model Law sets limitations on what qualifies as a cybersecurity event that materially diverge from the NYDFS cybersecurity regulation. Specifically, the Model Law does not cover unsuccessful attempts to access nonpublic information[3] and covers unauthorized acquisitions of encrypted nonpublic information only if the decoding key is also acquired. While diverging from the NYDFS approach, the Model Law is generally consistent with many state data breach notification laws that exclude unauthorized access to encrypted information from notification requirements.

Fourth, while a drafting note indicates that the drafters intend compliance with the NYDFS cybersecurity regulation to satisfy a licensee's obligations under the Model Law, the text of the Model Law does not contain an express exemption for licensees already subject to the NYDFS regulation, and it is unclear whether states will require additional documentation, or even a certification, to demonstrate that a licensee is in compliance with the NYDFS cybersecurity regulation.

Fifth, the third-party servicer provider provisions under the Model Act are very similar to those requirements imposed by the Gramm-Leach-Bliley Act safeguarding rules, which may ease implementation for licensees. This is in contrast to the NYDFS regulation, which imposes new requirements. Furthermore, unlike the Model Act, a person can be both a covered entity and a third-party service provider under the NYDFS cybersecurity regulation.

Sixth, states are becoming more active in the area of cybersecurity, and this presents challenges for companies engaged in a 50-state business. Over the past year, we have seen states, such as New York and Connecticut, impose cybersecurity requirements on insurance companies.[4] In the broker-dealer and investment adviser area, we have seen states, such as Colorado and Vermont, impose security requirements on certain types of entities. This development is similar to how the state data breach statutes evolved first with California, and now 48 states and the District of Columbia. Ultimately, this can lead to a complex patchwork of states laws, which increases the cost of compliance with these laws.

Seventh, the international community is also becoming more active in the area of cybersecurity, and this presents challenges for cross-border insurance groups. In 2016, the International Association of Insurance Supervisors (IAIS) released a whitepaper highlighting cyber-related issues in the insurance sector.[5] IAIS officials subsequently announced that they expect to develop a global cyber insurance standard, which may take the form of a new insurance core principle. It is likely that this standard will incorporate substantial content from the NAIC Model Law, but it is equally likely that a global standard may emphasize non-U.S. law priorities, such as greater customer control of data usage.

Lawrence R. Hamilton is a partner in Mayer Brown LLP's Chicago office and head of the firm's U.S. insurance regulatory practice.

Jeffrey P. Taft is a partner in the firm's Washington, D.C., office.

Matthew Bisanz is an associate in the firm's Washington, D.C., office.

Evan Sippel-Feldman is an associate in the firm's Palo Alto, California, office.

[1] NAIC, NAIC Passes Insurance Data Security Model Law (Oct. 24, 2017). The text of the Model Law, which has been designated by the NAIC as Model 668, is available at http://www.naic.org/store/free/MDL-668.pdf.

[2] NYDFS, Cybersecurity Requirements for Financial Services Companies, XXXIX (No. 9) N.Y. Reg. 3 (Mar. 1, 2017) (codified at N.Y. Comp. Codes R. & Regs. tit. 23, pt. 500). See our Legal Update on the NYDFS cybersecurity regulation.

[3] While the NYDFS cybersecurity regulation includes unsuccessful attempts in the definition, a subsequent FAQ issued by the NYDFS indicates that "most unsuccessful attacks will not be reportable, but seeks the reporting of those unsuccessful attacks that, in the considered judgment of the Covered Entity, are sufficiently serious to raise a concern." http://www.dfs.ny.gov/about/cybersecurity_faqs.htm.

[4] Connecticut's insurance laws require certain entities engaged in a health insurance business to maintain a comprehensive information security program and to certify compliance to the Connecticut Insurance Commissioner by October 1, 2017, and annually thereafter. Conn. Gen. Stat. § 38a-999b.

[5] IAIS, Issues Paper on Cyber Risk to the Insurance Sector (Apr. 14, 2016).