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

# Licensed by Your State's Insurance Commissioner? Comprehensive Data Security Requirements Are Headed Your Way

Article By:

Joseph J. Lazzarotti

Most businesses in the insurance industry have one thing in common – they collect and maintain significant amounts of sensitive, nonpublic information including personal information. Not surprisingly, insurance-related businesses are a target of cyberattacks and a few have faced some of the largest data breaches reported to date. Beyond the headlines, however, small and mid-sized insurance companies face similar risks, and governments have stepped up their scrutiny of cybersecurity. Hearing the calls for legislation and regulation, the National Association of Insurance Commissioners (NAIC) adopted a Data Security Model Law with the goal of having it adopted in all states within a few years. So far, eight states have adopted a version of the Model Law and it looks like more are on the way.

## What is the NAIC's Data Security Model Law?

In an effort that largely began with establishing a task force in 2014, the NAIC adopted a Data Security Model Law in November 2017. The Model Law is intended to provide a benchmark for any cybersecurity program. The requirements in the Model Law track some familiar data security frameworks, such as the HIPAA Security Rule. It also has many similarities to the New York State Department of Financial Services (NYDFS) regulations (specifically the 23 NYCRR 500). Note that licensees are not subject to the Model Law unless the state where that licensee is licensed adopts a version of the Model Law. At that time, the licensee must comply with that law.

## Who is Subject to the Model Law?

The Model Law generally applies to "Licensees," defined as:

any person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this State but shall not include a purchasing group or a risk retention group chartered and licensed in a state other than this State or a Licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction.

Licensees range from large insurance carriers to small independent adjusters. These include

individuals providing insurance related services, firms such as agency and brokerage businesses, and insurance companies. Additionally, there may be business that require a license, but are not traditionally considered to be in the insurance business. Examples include car rental companies and travel agencies that offer insurance packages in connection with their primary business.

The Model Rule provides exceptions for certain licensees. For example, licensees with fewer than ten employees (including independent contractors) are exempt from the requirement to maintain an information security program. However, they remain subject to the other provisions in the Model Law, such as the requirement to provide notification in the case of certain cybersecurity events.

## What are some of the requirements of the Model Law?

Under the Model Law, licensees must maintain a comprehensive, written “Information Security Program.” The Program should be commensurate with the size and complexity of the licensee, the nature and scope of the licensee’s activities, including its use of third-party service providers, and the sensitivity of the nonpublic information collected, processed, and maintained by the licensee. The Program also must be based on a risk assessment and contain administrative, technical, and physical safeguards. In short, the Program cannot be an “off-the-shelf” set of policies and procedures.

Some of the more specific requirements for a Program include:

- Make risk-based determinations on the security controls that should be implemented.
- Ensure the licensee’s Board or executive management carries out oversight of compliance.
- Exercise due diligence concerning data security in the selection of third-party service providers, and require third-party service providers to maintain reasonable safeguards.
- Maintain an incident response plan, and notify the insurance commissioner of a cybersecurity event within 72 hours.

## Does the Model Law Only Protect Personal Information.

No. The Model Law seeks to protect “nonpublic information,” which casts a wider net than, for example, personal information as defined under all state breach notification laws. Nonpublic information includes business related information of a licensee that if tampered with, or if there is an unauthorized access, use or disclosure, would cause a material adverse impact to the licensee’s business, operations or security. Of course, the Model Law also protects personal information defined to include a consumer’s identifying information in combination with one or more of the following: (i) Social Security number, (ii) driver’s license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to a consumer’s financial account, or (v) biometric records. The definition also includes certain health information concerning a consumer that relates to the consumer’s physical, mental or behavioral health or condition, the provision of health care, or the payment for the provision of health care.

## What States Have Adopted the Model Law?

South Carolina was the first state to adopt the Model Law when its Governor, Henry McMaster, signed the law on May 3, 2018. Ohio and Michigan followed in December 2018. On April 3, Mississippi Governor Phil Bryant signed that state's version of the Model Law, Senate Bill No. 2831, into law. Alabama followed in May. More recently, Delaware enacted a version of the Model Law, the Insurance Data Security Act, on July 31, 2019. Just prior to that, on July 26, 2019, Connecticut Governor Ned Lamont adopted its own version. Earlier this month, New Hampshire Governor Chris Sununu signed into law SB 194, which takes effect January 1, 2020 (although licensees have one year from the effective date to implement relevant cybersecurity requirements and two years to bring their third-party vendors into compliance). These laws have varying effective dates from January 1, 2019 through 2021. Legislation to enact a version of the Model Law has been introduced other states such as Nevada and Rhode Island.

Thus, to date, there are eight states that have enacted a version of the NAIC's Model Law. The laws are similar, but there significant differences. For example:

- The breach notification deadline in the NAIC's Model Law is 72 hours, however, it is 3 business days in Ohio and Delaware, and 10 days in Michigan. The Connecticut changed the existing 5-day rule under Insurance Department Bulletin IC-25 to no later than 3 business days.

- The NAIC's Model Law exempts smaller licensees, those with fewer than 10 employees and independent contractors, from the information security program requirement. States that have adopted the Model Law have change that exception. For example, Michigan increase the number to fewer than 25 employees and independent contractors. In Connecticut, licensees with fewer than 20 employees are excepted prior to September 30, 2021. After that, the exception drops down to fewer than 10 employees.

## What Should We be Doing?

Insurance businesses should be tracking these developments, particularly those that operate in multiple states. A good rule of thumb is to the adopt the most stringent aspects of the applicable laws into one compliance program. For businesses in states that have not yet enacted a version of the Model Law, your state may already have a generally applicable data security law requiring the business to maintain reasonable safeguards to protect personal information. See, e.g., Colorado and Massachusetts.



National Law Review, Volumess IX, Number 221