Radar® Privacy

INDUSTRY REPORT

Understanding the NAIC Insurance Data Security Model Law

Provisions, State-by-State Adoptions, and Notifications

In June of 2021, RadarFirst published a blog about the rapid rate of adoption of NAIC Model Laws. In the year since, the number of states that have passed data laws based on the NAIC model has more than doubled (rising from 10 states to 21 at the time of this writing).

Table of Contents

What is the NAIC?

State governments, not federal agencies, have preeminence over the insurance industry (as defined by the McCarran-Ferguson Act of 1945). Thus, it is up to each state to pass and enforce laws governing insurance companies. Each state has its own chief insurance commissioner to manage this function.

To create a consistent set of standards for state-by-state regulation of the industry, the 50 state insurance commissioners, along with one from the District of Columbia and five from U.S. territories, joined together to form the National Association of Insurance Commissioners (NAIC). This organization provides regulatory support to the individual states and territories by offering model laws that can be adopted wholesale by a state legislature, or modified to accommodate unique state-by-state differences.

The NAIC drafts model laws for states governing many aspects of the insurance industry. When RaderFirst writes about the NAIC Model Law, we refer specifically to the Insurance Data Security Model Law (MDL 668).

Introduction to the NAIC Model Law

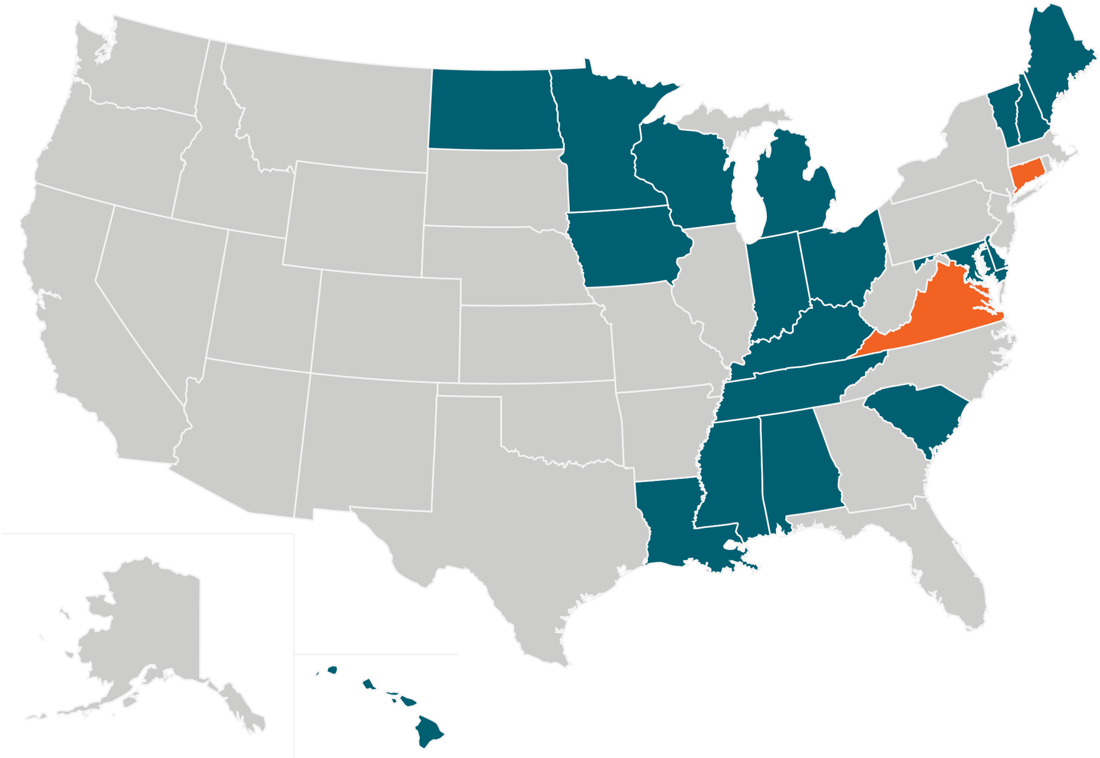
The NAIC Model Law (Model Law)—known formally as the Insurance Data Security Model Law—was written by the National Association of Insurance Commissioners (NAIC) to serve as a model for each U.S. state, district, and territory to use in drafting its own legislation governing how the insurance industry will safeguard and manage individual customer data.

The NAIC saw a need for this law as a response to the growing number of large insurers experiencing data breaches. Providing a mechanism for state governing bodies to address consumer needs and concerns was a way to forestall federal intervention in the industry in response to those breaches.

Since 2017, when it was finalized, the Model Law–or a modified version thereof–has passed in 21 states.

States Who Have Adopted NAIC

List of states that have passed NAIC Model Laws as of this writing:



- **Alabama**
- **Connecticut**
- **Delaware**
- **Hawaii**
- **Indiana**
- **Iowa**
- **Kentucky**
- **Louisiana**
- **Maine**
- **Maryland**
- **Michigan**
- **Minnesota**
- **Mississippi**
- **New Hampshire**
- **North Dakota**
- **Ohio**
- **South Carolina**
- **Tennessee**
- **Vermont**
- **Virginia**
- **Wisconsin**

States with NAIC Model Laws passed

States with both Comprehensive Data Security Laws and NAIC Model Laws

NAIC Calls for Urgent Adoption to Forestall Federal Government Intervention

The existence of pre-vetted language specifically designed to govern the insurance industry's use of data has meant that these NAIC Model Laws tend to move through the state legislatures more quickly than comprehensive cybersecurity laws, which can spend years in back-and-forth revisions and negotiations. As of this writing, only five states have passed a comprehensive set of Privacy Bills, while 21 have passed data laws specifically relating to the insurance industry.

In addition to the relative efficiency of adopting pre-vetted legislation, the pace of adoption of the Model Law has been spurred on due to a report issued by the U.S. Treasury Department in October 2017. In the report, the U.S. Treasury urged prompt action by states to adopt the NAIC Model Law within five years. If the Model was not adopted and implemented widely, the report recommended that Congress act by passing legislation setting forth uniform requirements for insurer data security.

As the clock winds down on the five-year recommended adoption period, companies should expect to see more states and districts adopt the NAIC Model Law in the second half of 2022.

Understanding Data Incident Management Provisions in the NAIC Model Law

While the NAIC Model Law goes into depth about all aspects of managing and protecting data, for the purposes of this white paper, we will focus only on the major provisions related to Data Incident Management and Notification. The Model Law provides several key aspects for incident response, including:

Notification Window

The notification window refers to how long an organization has to notify the State Insurance Commissioner after confirming that an incident occured. The Model Law as written requires notification, "as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred." The law goes on to detail the conditions that define an event based on whether the insurance provider, the impacted consumer(s), or both, are domiciled in the state.

Threshold for Notification

The Model Law requires notification to the office of the State Insurance Commissioner (and other applicable oversight bodies as required by law) as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred when either of the following criteria has been met:

- **(1) This State is the Licensee's state of domicile; or**
- **(2) The Licensee reasonably believes that the Nonpublic Information involved is of 250 or more Consumers residing in this State and that is either of the following:**
  - **(a) A Cybersecurity Event impacting the Licensee of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body pursuant to any state or federal law; or**
  - **(b) A Cybersecurity Event that has a reasonable likelihood of materially harming: (i) Any Consumer residing in this State; or (ii) Any material part of the normal operation(s) of the Licensee.**

Notification Content

The Model Law details 13 separate categories of information that must be considered in the notification to the Commissioner.

Data Breach Incident Information Required by NAIC Model Law

- **Date of the event**
- **Description of how information was exposed, including the roles of third-party service providers**
- **How the cybersecurity event was discovered**
- **Whether any lost, stolen, or breached information has been recovered and if so, how**
- **Identity of the source of the cybersecurity event**
- **Whether Licensee has filed a police report or notified regulatory, government or law enforcement agencies and, if so, when**
- **Description of the specific types of information acquired without authorization**
- **Period during which the information system was compromised by the cybersecurity event**
- **Number of total consumers in the state affected by the event**
- **Results of internal review identifying a lapse in automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed**
- **Description of efforts being undertaken to remediate the situation which permitted event to occur**
- **Copy of the licensee's privacy policy and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the cybersecurity event**
- **Name of a contact person who is familiar with the event and authorized to act for the licensee**

> *All data breach incident information required by the NAIC Model Law (and more) is tracked in the Radar® Privacy incident management platform to help businesses comply with notification requirements on a state-by-state basis.*

Who Must Be Notified

The Model Law requires a notification be sent to the State Insurance Commissioner, as well as any other governing bodies required by other state legislation on the books. The Model Law leaves the determination of whether to notify individual consumers up to the state's individual adoption of the law, with some states including a specific requirement to notify consumers, while others leave the requirement under the state's data breach notification law.

Other incident response topics the Model Law addresses include:

- **How to handle incidents impacting third party service providers**
- **How to handle incidents impacting reinsurers**

Click here to read the NAIC Model Law in full.

Nuances in Data Incident Management Requirements Vary by State

While in theory, the NAIC Model Law provides a standardized approach to governing how companies must manage and respond to data incidents. In practice, we have seen that state-by-state, enacted laws are full of notable variances from the Model, reflecting the distinct preferences and business climates of individual states.

When it comes to incident management and response, the nuances that are particularly important to note within the laws include: differences in the notification window, differences in the threshold for notification, the types of consumer information that – if breached – would be considered a data incident, the individuals and oversight bodies that must be notified, and as mentioned above, whether and in what circumstances consumers must be notified.

Data points such as state, effective date, and notification window are only three of 18 categories of compliance the Radar® Privacy automated platform tracks and uses to determine incident risk.

Unlike other state laws Vermont's H.515 does not impose notification obligations on licensees following a cybersecurity event. Instead, licensees are bound by the notification requirements of the Vermont Security Breach Notice Act, 9 V.S.A. § 2435.

Additionally, some adoptions of Model Laws specify a different notification threshold for domiciled and non-domiciled insurers or if notice is required to another regulatory body, adding in more challenges for insurers or producers who operate in multiple jurisdictions in designing their compliance programs to accommodate varying obligations.

State	Date Effective	Notification Requirements
Alabama	May 1, 2019	3 business days
Connecticut	April 19, 2021	3 business days
Delaware	July 31, 2019	72 hours (3 days)
Hawaii	July 1, 2021	3 business days
Indiana	July 1, 2021	3 business days
Iowa	Jan 1, 2022	3 business days
Kentucky	Jan 1, 2023	3 business days
Louisiana	Aug 1, 2020	3 business days
Maine	Jan 1, 2022	3 business days
Maryland	Oct 01 2022	3 business days
Michigan	Jan 20, 2021	10 business days
Minnesota	Aug 1, 2021	5 business days
Mississippi	July 1, 2019	3 business days
New Hampshire	Jan 1, 2020	3 business days
North Dakota	March 23, 2021	3 business days
Ohio	March 20, 2019	3 business days
South Carolina	Jan 1, 2019	72 hours (3 days)
Tennessee	July 1, 2021	3 business days
Vermont	Jan 1, 2023	72 hours (3 days)
Virginia	Jul 1, 2020	3 business days
Wisconsin	Nov 1, 2021	3 business days

> *"Nuances within NAIC Model Law adoptions means that insurance licensees will find it challenging to apply a simple, uniform set-it-and-forget-it compliance policy. It also means that automation of privacy incident risk assessment could be considered a basic business necessity to maintain compliance with evolving laws."*
>
> –Lauren Wallace, Chief Privacy Officer and General Counsel, RadarFirst

Notification Windows Range from 72 Hours to 10 Days

A detailed review of state-adopted versions of the NAIC Model Law shows that the notification window for a cybersecurity event ranges from 72 hours (the Model guideline), to three "business days," to 10 business days in some cases.

In states where other consumer data breach notification laws are in place, of course, responding to an incident is further complicated by the fact that **those additional laws may specify a completely different set of notification windows.**

The likelihood that many states will pass their own comprehensive cybersecurity laws in the next few years will undoubtedly add further complexity. Without an automated response system, companies will find it extremely difficult to meet deadlines and avoid penalties.

Differing Definitions of Nonpublic (Consumer) Information

The Model Law sets forth the definition of information that would be considered nonpublic as follows:

1. **Business-related information that if released would cause material harm to the licensee.**
2. **Consumer data in which a name, number, or other personal mark or identifier is combined with any of the following: Social Security number, driver's license or ID number, account numbers, or security codes or passwords.**
3. **Health and mental health data or treatment data, or payment data relating to health or mental health data of the individual or a family member.**

While most states have adhered to these definitions when adopting the NAIC Model Law, a few notable exceptions include states that do not include business-related information and a state that has added military IDs and passport numbers to its list of nonpublic consumer data.

These existing exceptions suggest that other states will continue to adapt the definition as they pass their own NAIC Model Laws. **An automated risk assessment tool will be instrumental in understanding which data is implicated in each jurisdiction.**

Widely Varying Requirements Regarding Whom to Notify

As mentioned above, the NAIC Model Law mandates that notification of an incident be made to the State Insurance Commission and also to any other governing bodies named in any other relevant legislation. Further, the question of whether or not to notify consumers is left to the states based on whether other cybersecurity laws are in place.

Because nearly every state has a different slate of laws on the books governing individual industries, data formats, and incident types, it is a foregone conclusion that every state with adapted NAIC Model Laws will have a different set of notification and reporting obligations. **A response platform that tracks required notifications, as well as a module to customize the notifications according to state requirements will save days, if not weeks, of work.**

Compliance Grace Periods Add Further Nuance

The NAIC Model Law suggests that companies have up to a year following the law's enactment to develop and implement an information security program (which must be delivered to the State Insurance Commission). On top of that, the Model Law allows for another year to develop a program for data managed, used, or stored by third-party providers. States are likely to determine their own compliance timelines, but even if they do not, the Model timeline is already complex.

Taken in full, the nuances inherent in complying with NAIC Model Laws state-by-state drive the pressure on privacy teams higher and higher.

Predictions for Data Incident Management Response and the Insurance Industry Moving Forward

With only a few months until the federal government's recommended adoption and implementation period ends, Radar® Privacy anticipates that many states will enact NAIC Model Laws in the second half of 2022.

However, privacy teams should not consider any new legislation to be a one-and-done set of guidelines. The NAIC is currently reviewing and updating the NAIC Model Law discussed in this white paper (MDL 668), as well as Model Law 672 Privacy of Consumer Financial and Health Information Regulation.

Organizations should expect that when NAIC issues the new language for these laws, states will respond with amendments to their already adopted NAIC Model Laws, resulting in a constantly shifting set of requirements for incident management and response.

Privacy teams that rely on manual, one-size-fits-all incident response processes or that have previously found success tracking new laws manually will need to make the transition to automated risk assessment and intelligent incident management software platforms in order to keep up with the nuances and complexities required on a state-by-state basis.

Learn how Radar® Privacy's automated risk assessment and intelligent incident response software platform can help you usher in Digital Transformation of your data privacy and security processes.

Companies that demonstrate a commitment to creating a culture of responsible and responsive data management – including a strong infrastructure of digital tools to automate their processes for on-time, complete incident responses – will likely fare better when facing the inevitable data breach.

Enforcement Measures Will Focus on Compliance, Consumer Awareness

In most states, insurance companies have a period of eight months to a year between the law's passage and the law going into effect to develop their data plan, so it is likely we will begin to see enforcement measures in states that are one year or more past the post.

State enforcement of NAIC Model Law provisions may look much like enforcement practices for other insurance industry noncompliance.

In general, the NAIC describes enforcement as a process of investigations, recommendations to bring the company into compliance, and if called for, a combination of civil penalties, license suspension, or license revocation.

For example, a data breach incident in Texas affected the state's own office for worker's compensation insurance. The state agency's response included:

- **Working with a forensic company to investigate the nature and scope of the event**
- **Reviewing and enhancing policies, procedures, and security efforts**
- **Offering 12 months of credit monitoring and identity protection services at no cost to those who may have been affected**
- **Providing a dedicated helpline for questions about the event**

State Insurance Commissioners have yet to set precedents on what kind of civil penalties might be levied, but state laws mention penalties ranging from $100 to $150,000 or more if companies failed to act on known weaknesses in their data management plan. Most states do not allow consumers private right of action, but a few exceptions exist, specifying actual damages only.

Companies Will Use Data Incident Benchmarking as Decision Intelligence

As companies automate their data incident management and response, they will be able to put data breaches to work for them, allowing their privacy teams to make better decisions, differentiating their companies among competitors in the industry.

The Radar® Privacy Guide to Digital Transformation for Privacy Incident Management made the case that in order to reap the benefits of digital transformation, your organization must have decision intelligence. According to Gartner, which coined the term, ***decision intelligence comes from the integration of data, analytics, and automation to create platforms to support, augment, and automate decisions.*** In other words, decision intelligence is the ongoing, automated, analyzed data you need to make strategic business decisions.

Decision intelligence allows your organization to:

- **Evaluate historic decisions and processes for improvements**
- **Create employee awareness training to change practices and processes**
- **Run models to drive future decisions**
- **Identify response processes across the organization that could be simplified or, better yet, automated**

The Radar® Privacy Intelligent Incident Management Platform gives you the ability to automate your data processes, collaborate and communicate across teams, and benchmark your incident management and response activities, generating an ongoing source of decision intelligence for your company.

Approach to Data Incident Management and Response Will Become an Intangible Asset in the Valuation of a Company

As companies begin to differentiate themselves based on their approach to data management and incident response practices, cybersecurity competencies will become a valued component of brand identity. More states will likely follow Texas's lead in maintaining a public list of companies who have had data breach incidents, as well as how the companies reacted.

Customers will make purchasing decisions based on the strength and responsiveness of data incident response, and analysts and investors will assign monetary value to a company's commitment to digital transformation of data management and incident response. A company's position in mergers and acquisitions will be directly impacted by their cybersecurity profile.

Digital Transformation of Data Incident Management and Response Will Be Critical to Meeting Complex Requirements

The complex legal framework governing data management in general, and data within the insurance industry specifically, has grown to the extent that manual tracking and response will be nearly impossible in the very near future (if not already).

Privacy leaders and teams require robust, third-party software platforms to avoid over- or under-notifying governing agencies and consumers, and to avoid incurring civil penalties, or worse yet, suspension or revocation of a license to act as an insurance provider.

The Radar® Privacy Intelligent Incident Management Platform provides flexible, reliable capabilities to comply with new state adoptions of the NAIC Insurance Data Security Model Law. In real-time, Radar® Privacy:

1. **Determines if the incident qualifies as a notifiable cybersecurity event**
2. **Provides a jurisdiction-by-jurisdiction risk of harm analysis**
3. **Alerts you of notification timelines for each jurisdiction**
4. **Enables quick outreach with notification templates**
5. **Publishes state-specific law overviews to support your understanding of a law's complexity**

We track new laws and amendments to existing laws, keeping our automated platform up-to-date, which means your business can feel confident that it is maintaining best practices in data incident management and response. As a result, consumer and market confidence in your brand will grow. The need for transforming your data practices to make use of the latest technology solutions has never been more vital for your business.

Radar® Privacy

Digitally Transform your Incident Management with Radar® Privacy today.

INFO@RADARFIRST.COM | 1.844.737.3778

Schedule a Demo

Additional Resources

- 2023 Privacy Incident Benchmark Report »
- The Digital Transformation Guide for Privacy »
- See Radar® Privacy in Action: Learn how you can streamline incident intake, automate risk assessment, and simplify notification compliance today. Schedule a Demo »

RadarFirst

Learn more at radarfirst.com

RadarFirst's award-winning incident management platform is trusted by organizations in heavily regulated industries to reduce risk and simplify compliance with global data breach laws.