

NAIC DATA SECURITY MODEL LAW.



The NAIC Model Law only becomes real once a state enacts it — a licensee's actual obligations are set by a patchwork of individual state statutes, not a single uniform national rule.

- STATE-BY-STATE ADOPTION
- LICENSEE INFORMATION SECURITY PROGRAM
- THIRD-PARTY VENDOR DILIGENCE
- 72-HOUR COMMISSIONER NOTIFICATION

01 THE MECHANISM

Model Law, Not Automatic Law

NAIC develops and recommends the Model Law, but **it only takes effect in a state once that state's own legislature enacts it** — until then, insurance licensees there aren't bound by it at all.

Licensee Scope via State Insurance Law

Any person or entity licensed, authorized, or registered under a state's insurance law — carriers, agents, brokers, MGAs — falls under an adopting state's version of the law, **using the same broad licensing hook** as NYDFS's covered-entity definition.

Limited Small-Licensee Exemption

Licensees below defined size thresholds, and those already compliant with HIPAA or covered under another licensee's program, can qualify for exemption — **but it's narrow, not a blanket carve-out** for small insurance businesses.

02 THE FLOW

The Multi-State Compliance Program CONTAINED

1

The licensee tracks exactly which states it operates in have adopted the Model Law, and builds its information security program to the strictest adopted variant rather than guessing.

2

A designated individual owns the written information security program, with **risk assessments and vendor due diligence documented** the same way regardless of which state's version applies.

3

A qualifying cybersecurity event triggers **notification to every applicable state insurance commissioner** within that state's required window, not just the licensee's home state.

The Single-State Assumption EXPOSED

1

The licensee assumes its home-state compliance program automatically satisfies every other state it's licensed in, without checking which states have actually adopted the law or how their versions differ.

2

A cybersecurity event is reported to one state regulator, while **other states where affected consumers reside never receive their required notification**.

3

The information security program is built once for a single jurisdiction's threshold and **never revisited as new states adopt their own version** of the Model Law.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Written, Risk-Based Information Security Program	Requires an ISP appropriate to the licensee's size, complexity, and the sensitivity of the nonpublic information it handles, overseen at the board or senior-management level.
Periodic Risk Assessment	Requires identifying reasonably foreseeable internal and external threats on an ongoing basis, not as a one-time exercise at program launch.
Third-Party Service Provider Oversight	Requires due diligence on vendors handling nonpublic information, extending the licensee's own security obligations into its supply chain.
72-Hour Commissioner Notification	Requires notifying the state insurance commissioner within 72 hours of determining a qualifying cybersecurity event occurred, mirroring NYDFS's notification clock.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Home-State Program Applied Everywhere	No	Assumes uniform adoption across states when the Model Law is actually enacted state by state, with real variation in scope and thresholds between them.
One-Time Risk Assessment at Launch	No	Meets an initial checkbox but misses new threats, vendors, and business changes that emerge after the program was first built.
Vendor Contracts Without Security Due Diligence	No	Leaves the licensee's own compliance exposed to whatever security practices, or lack of them, a third-party processor actually follows.
Notify Only the Licensee's Home-State Regulator	No	Misses the separate notification obligation owed to every other adopting state where affected consumers or the incident meets that state's threshold.
State-by-State Tracking + Documented ISP + Vendor Diligence + Multi-State Notification	Yes	Treats the patchwork of adoption as the actual compliance surface, rather than assuming one program covers every licensed state.

NAIC DATA SECURITY MODEL LAW.

ADOPT · ASSESS · NOTIFY

05 PROGRAM OPERATIONS

Adoption is state-by-state, not automatic.

A licensee operating in multiple states must track each state's own enactment status and any variations from the NAIC's original model text.

The Model Law was built directly on NYDFS 23 NYCRR 500.

Its information security program, risk assessment, and notification structure closely mirror New York's earlier regulation.

Limited exemptions require checking the specific state's language.

Employee-count and HIPAA-related carve-outs exist, but their exact thresholds can differ between adopting states.

A single incident can trigger multiple states' notification clocks at once.

Affected consumers spread across adopting states each activate that state's own commissioner-notification requirement.

06 CONTROL MAPPING

NAIC INSURANCE DATA SECURITY MODEL LAW (MDL-668)

The model text NAIC recommends to states, covering information security programs, risk assessment, and incident notification for insurance licensees.

NYDFS 23 NYCRR 500

The New York regulation the Model Law was directly modeled on, sharing much of its structure and requirements.

STATE INSURANCE DATA SECURITY ACTS

Individual state enactments, such as South Carolina's 2018 Insurance Data Security Act, the first state to adopt the Model Law.

GLBA SAFEGUARDS RULE

The federal baseline for financial institution data security that predates and can overlap with a licensee's state-level obligations.

07 WHAT THIS DOES NOT SOLVE

Non-Adopting State Gaps

In states that haven't enacted the Model Law, a licensee's insurance-specific obligations under this framework **simply don't exist yet** — other laws may still apply.

Federal Regulatory Overlap

Compliance with a state's Model Law doesn't itself satisfy **separate federal obligations**, like GLBA or HIPAA, that may also apply to the same licensee.

Non-Cyber Solvency & Market Conduct Risk

An adequate information security program doesn't address **the insurer's separate solvency, reserving, or market-conduct obligations** under state insurance law.

Cross-Border Reinsurance & Global Operations

The Model Law binds licensees under state insurance law, but doesn't reach **ICT risk at foreign reinsurers or offshore operations** outside that licensing scope.

08 MYTHS VS. REALITY

MYTH

"The NAIC Insurance Data Security Model Law is federal law."

REALITY

It's a **model recommended by the NAIC**, an association of state regulators — it only becomes binding once an individual state's legislature actually enacts it.

MYTH

"Adopting the Model Law means every state's version is identical."

REALITY

States can and do **modify thresholds, exemptions, and specific requirements** when enacting their own version, so the same licensee can face different obligations state to state.

MYTH

"This is a completely separate framework from NYDFS."

REALITY

The Model Law was **explicitly built on NYDFS 23 NYCRR 500's structure** — most of its core program, assessment, and notification requirements will look familiar to anyone who has worked with the New York rule.

MYTH

"Small insurance agencies are automatically exempt."

REALITY

The small-licensee exemption applies only **below specific employee-count and other thresholds defined in each state's version** — it isn't a blanket exemption for small businesses generally.

MYTH

"One 72-hour notification to my home state covers the incident everywhere."

REALITY

A qualifying event can trigger **separate 72-hour notification obligations to every other adopting state** where affected consumers or thresholds apply, not just the licensee's home-state regulator.

09 SPEAK THE PROGRAM — KEY TERMS

MODEL LAW

A framework the **NAIC recommends to state legislatures**, which only becomes binding law in a given state once that state formally enacts it.

LICENSEE

Any person or entity **licensed, authorized, or registered under a state's insurance law** — carriers, agents, brokers, and managing general agents alike.

INFORMATION SECURITY PROGRAM (ISP)

The **written, risk-based program** a licensee must maintain, sized to its own complexity and the sensitivity of the nonpublic information it holds.

STATE INSURANCE DATA SECURITY ACT

The **name typically given to a state's own enactment** of the NAIC Model Law, such as South Carolina's, the first state to adopt it in 2018.

72-HOUR NOTIFICATION

The requirement to notify a state's insurance commissioner within **72 hours of determining a qualifying cybersecurity event occurred**, mirroring NYDFS's own notification clock.

LIMITED EXEMPTION

Reduced obligations for licensees below defined **employee-count or other size thresholds**, or already compliant with HIPAA or another licensee's program — a partial, not full, carve-out.