SmartSuite

Framework / Cybersecurity / Other

NAIC Insurance Data Security Model Law MDL-668 (2017)

The NAIC Insurance Data Security Model Law (#668) is the model act states enact to require insurers and producers to run a written security program and report events in 72 hours.



What it is

The NAIC Insurance Data Security Model Law (#668) is a model act, adopted by the National Association of Insurance Commissioners (NAIC) Executive Committee and Plenary on October 24, 2017, that states enact to require every insurer, producer and other licensee to run a written information security program, investigate cybersecurity events and notify the state insurance commissioner within 72 hours. It binds a licensee only through a state's own enactment; the NAIC reports 28 jurisdictions as adopted and one pending in its implementation map (status as of April 1, 2026).

At a glance

PUBLISHER
National Association of Insurance Commissioners (NAIC); enacted by each state legislature

TYPE
Framework

VERSION
NAIC Model #668 (adopted October 24, 2017; technical edit 2025)

EFFECTIVE
Varies by state; Section 13 gives one year from a state's effective date to implement Section 4 and two years for Section 4F

DOMAIN
Cybersecurity

FAMILY
Other

REGION
United States (state by state; 28 jurisdictions adopted as of April 1, 2026)

INDUSTRY
Insurance

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: content.naic.org/model-laws

Why it matters

- **A written program tied to a risk assessment** Section 4A requires a comprehensive written Information Security Program based on the Licensee's Risk Assessment, scaled to its size, activities and use of third parties.
- **Named security measures** Section 4D(2) lists measures to implement where appropriate: access controls, encryption of data in transit and on portable devices, multi-factor authentication, audit trails, secure disposal and testing.
- **Board and executive accountability** Under Section 4E the board or a committee requires management to report in writing at least annually on program status and compliance.
- **A 72-hour notice** Section 6A requires notice to the Commissioner within 72 hours of determining that a Cybersecurity Event occurred, when the listed criteria are met.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NAIC MDL-668

Section 4 Requirement Library

Load Sections 4A through 4I, including the Section 4D(2) measures, as requirements with owners, status and linked policies and evidence.

Risk Assessment Record

Keep the Section 4C assessment in Cyber & IT Risk with identified threats, likelihood and damage ratings, safeguards reviewed and the annual effectiveness check.

Service Provider Oversight

Record each Third-Party Service Provider's due diligence, required safeguards and event-notice terms under Section 4F in Third Party Risk Management.

Incident and Notice Workflow

Log each Cybersecurity Event with the determination date, a 72-hour deadline for Section 6A, the Section 6B content checklist and the state breach-law notice.

Board Report and Certification

Assemble the Section 4E annual report and the Section 4I February 15 certification from the same records, with remediation plans for areas needing improvement.

Five-Year Records

Retain event records (Section 5D) and certification support (Section 4I) for five years with dates and owners.

Common framework mappings

CIS Controls v8.1 · EU DORA · FFIEC IT Handbook · GLBA Safeguards Rule (16 CFR Part 314) · ISO 27001:2022 · NIST CSF 2.0 · NIST 800-53 Rev.5 · SOC 2

Official resources

NAIC Insurance Data Security Model Law (MDL-668)

Defines data security requirements for insurance entities to protect consumer information.

content.naic.org/model-laws/mdl-668

NAIC Cybersecurity Guidance

Provides implementation guidance for achieving compliance with the NAIC Cybersecurity Model Law.

content.naic.org/cipr_topics/cybersecurity.htm

Frequently asked questions

Who must comply with the NAIC Insurance Data Security Model Law?

The model itself binds no one; it applies to a Licensee in a state that has enacted it. Section 3I defines a Licensee as any person licensed, authorized or registered, or required to be, under the state's insurance laws. The NAIC's implementation map lists 28 jurisdictions as adopted and one pending as of April 1, 2026, and New York is shown separately under other insurance data security provisions.

When must a licensee notify the insurance commissioner of a cybersecurity event?

Section 6A requires notice as promptly as possible and no later than 72 hours after determining that a Cybersecurity Event occurred. Notice is due when the state is the insurer's domicile or the producer's home state, or when the Licensee reasonably believes the Nonpublic Information of 250 or more state residents is involved and notice is required elsewhere or the event is reasonably likely to cause material harm. Section 6B lists the 13 items to report and requires updates.

What is the annual certification in Section 4I?

Each insurer domiciled in the state submits a written statement to its Commissioner by February 15 certifying compliance with Section 4. The insurer keeps all supporting records, schedules and data for five years for examination. If it has found areas needing material improvement, it documents the issue and the remedial efforts planned and underway.

Who is exempt under Section 9?

A Licensee with fewer than ten employees, including independent contractors, is exempt from Section 4. A HIPAA-covered Licensee that maintains a compliant information security program is considered to meet Section 4 if it submits a written statement certifying compliance. An employee, agent or designee covered by another Licensee's program is also exempt, and a Licensee that stops qualifying has 180 days to comply.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How long do licensees have to implement it, and how does it relate to New York's cybersecurity rule?

Section 13 gives licensees one year from a state's effective date to implement Section 4 and two years to implement the Section 4F oversight of Third-Party Service Providers. The drafting note to Section 2 states the drafters' intent that a licensee in compliance with 23 NYCRR 500, effective March 1, 2017, is also in compliance with the model.

License included / downloadable: Yes The Insurance Data Security Model Law is published free by the NAIC as a PDF on its Model Laws page; the platform links to the official text and does not reproduce it.

Full framework page and mappings: smartsuite.com/frameworks/naic-insurance-data-security-model-law-mdl-668-2017