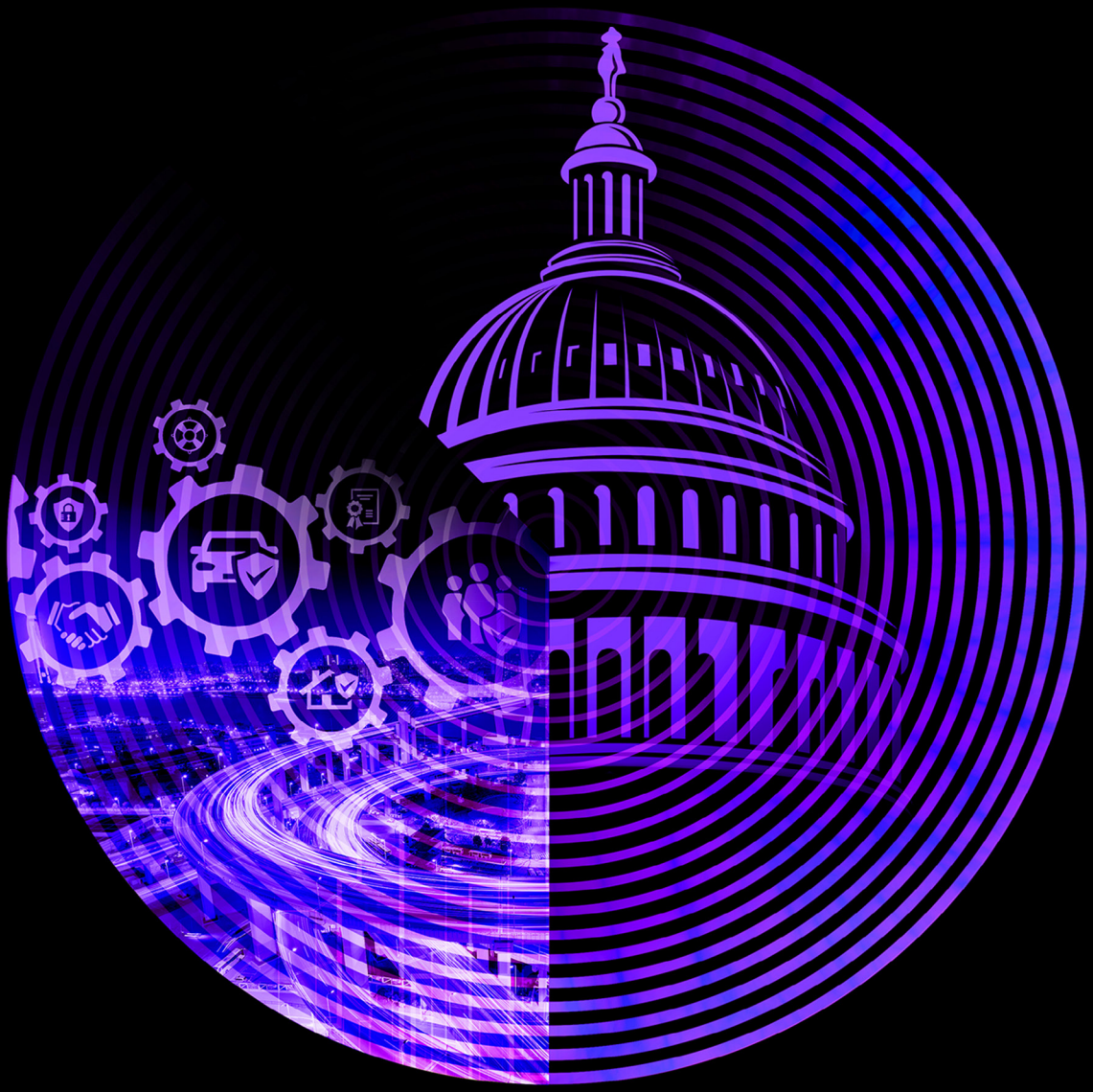
Deloitte.

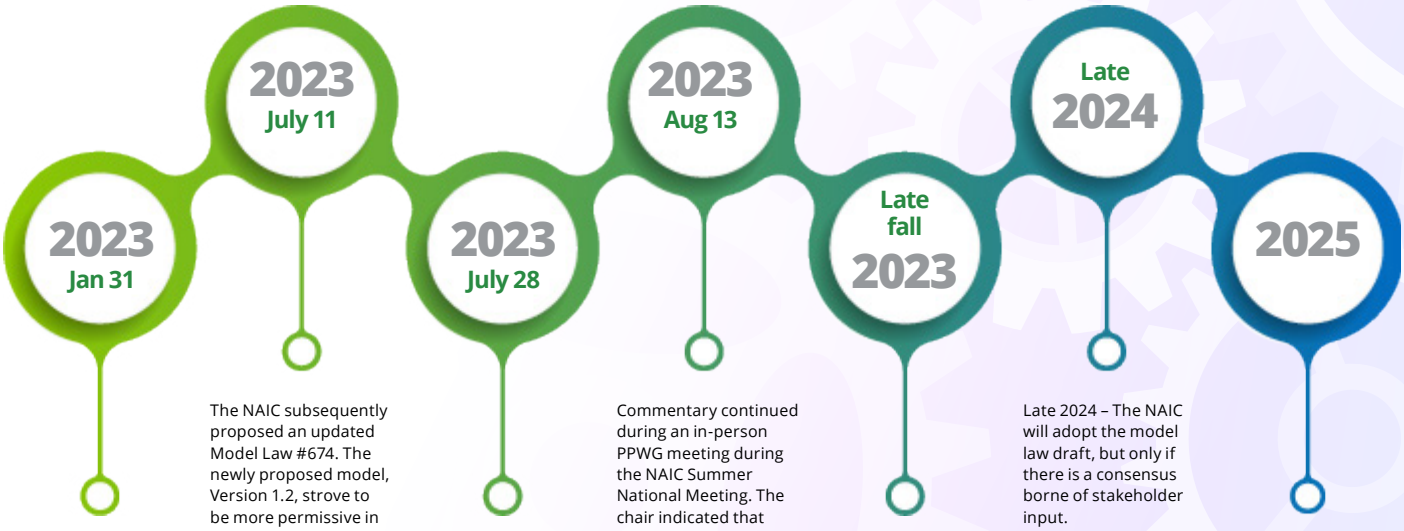


NAIC's Consumer Privacy Protection Model Law #674

Center *for*
Regulatory Strategy US

Introduction

NAIC's Insurance Consumer Privacy Protection Model Law #674 is again in the spotlight. Version 1.2 will face a redline reckoning, and firms should prepare for a final draft that could be adopted by state legislatures. Firms should consider developing an action plan through the review of proposed regulations, assessing their existing data governance processes and identifying potential enhancements.



2023 Jan 31

A draft of the National Association of Insurance Commissioners (NAIC) Insurance Consumer Privacy Protection Model Law #674 was first introduced. During the NAIC Spring 2023 National Meeting in Louisville, the Privacy Protection Working Group (PPWG) concluded, following commentary from stakeholders in the industry, that the first draft was simply unworkable and could not go forward as originally drafted.[1]

2023 July 11

The NAIC subsequently proposed an updated Model Law #674. The newly proposed model, Version 1.2, strove to be more permissive in some respects than the previous model, such as on joint marketing and opt-in/opt-out language, yet is still viewed as significantly problematic in language and intent in its current form by some influential industry participants and others, although consumer advocates indicated their overall support for it.[2]

2023 July 28

Comments on Version 1.2 were due.

2023 Aug 13

Commentary continued during an in-person PPWG meeting during the NAIC Summer National Meeting. The chair indicated that the group will review voluminous comments on the existing version, create a new version with a new four-to-six week comment period, and then have a "better idea" for how much of an extension will be needed.[3]

A redlined version will be published after the PPWG processes all the comment letters and feedback from private and public meetings. There will be four to six weeks for comments on the new, redlined version.

Late fall 2023

The draft, due to the extension, will likely not be ready for adoption by its parent committee, the Innovation, Cybersecurity and Technology (H) Committee, during the NAIC Fall National Meeting. Once a draft has been adopted by the PPWG, it will go before the parent committee, which could happen by spring 2024 if the process stays on course.[4] The Working Group in August 2023 underscored the fact it needs more time to engage the public and continue with its drafting of the model.

Late 2024

Late 2024 – The NAIC will adopt the model law draft, but only if there is a consensus borne of stakeholder input.

2025

State legislatures can consider adoption once a model law is adopted by the NAIC Executive Plenary.

Version 1.2 key features on sharing of information and third-party use

How insurers deal with third parties will be under scrutiny by insurance supervisors, but the extent to which insurers must oversee them and be able to share information with state regulators during market conduct exams or in other oversight events or dialogue will continue to be crafted and fine-tuned, although Version 1.2 points the way, for now. Consumer protections remain top of mind for state regulators in the new draft. The PPWG tried to ease restrictions on data retention and sharing information, as well. The latest draft:

- Provides consumers with rights around personal and publicly available information in the possession of the licensee or its third-party service providers.
- Prevents insurers from allowing third-party service providers to collect, process, retain, or share any consumer's personal information in any manner contrary to the model and the licensee's own privacy protection practices.
- Clarifies that "third-party service provider does not include a licensee's 'affiliates.'"
- A licensee must exercise due diligence in selecting its third-party service providers.
- Requires that a written contract between the licensee and third-party service provider be in place for a licensee to engage a third-party service provider to collect, process, retain, or share any consumer's personal information with a third-party service provider for any purpose.
- No longer prohibits cross-border sharing of consumers' personal information. The model would only require notice to consumers that such information is processed or shared in this manner.
- Attempts to address the industry's concerns on deletion of personal information from legacy systems.
- Adds a provision to permit joint marketing agreements.
- Allows consumers to opt out of marketing, with opt-in provisions narrowed.
- Publicly available information can be shared by a licensee with a third-party service provider without a written contract only if it is in connection with a claim, and then only to the extent necessary to provide the service requested by the consumer.
- Strengthens the language on confidentiality but does not adopt the NAIC's Own Risk and Solvency Assessment (ORSA) language.

A deeper dive into key changes

Stakeholders went further to express their opinions on how the draft deals with data deletion from legacy systems, transition time for changes, joint marketing language, and the regulatory language crafted to address omnipresent and growing interplay with third-party vendors.

- Industry indicated that the process of deletion of personal information from legacy systems is costly and takes years to transition. Thus, Version 1.2 would require a licensee to review its retention policy and all consumers' personal information in its possession annually to determine whether personal information should be retained. If no longer needed, the licensee must delete all the consumer's personal information within 90 days.

  If targeted disposal is not feasible, the licensee must de-identify the information to the extent possible under approval from the regulator. If it cannot be deleted or de-identified, the licensee must develop a written data minimization plan that provides for transition from such system within a reasonable time frame.

  Version 1.2 asserts that there must be a reasonable effort to transition from legacy systems. Licensees retaining consumers' personal information on systems where targeted disposal is not feasible must de-identify all such information to the extent possible, subject to approval from the insurance commissioner. Additionally, the licensee must annually report in detail the licensee's progress for such transition to its domestic regulator. Consumer advocates have expressed misgivings with the permitted time frames as being too lengthy.[5]

- In order to share a consumer's personal or publicly available information in a joint marketing agreement, the draft states that the consumer must first be provided a clear and conspicuous means to opt out of sharing, be given reasonable time to opt out of the sharing, and receive a notice that includes a description of the right to opt out for marketing reasons.
- Any consumer can submit a verifiable request to the licensee for access to the consumer's personal and publicly available information in the possession of the licensee or its third-party service providers. The licensee or third-party service provider must acknowledge the request within five business days and provide a required response within 45 business days. The response must be detailed: It must include the identity of those consumers whose personal information has been shared within the current year and three calendar years prior to the date the consumer's request is received—at a minimum; provide a summary of personal information and process for consumer to request a copy of such information in possession; and identify the source of any consumer's personal information provided.
- Contracts must honor the consumer's directive, whether it is an opt-in or an opt-out, and refrain from collecting, processing, retaining, or sharing the consumer's personal information in a manner inconsistent with the directive of the consumer.

The draft AI bulletin adds to third-party vendor involvement from licensees in measures

In addition to insurer oversight of third-party service providers required by Version 1.2, insurance regulators also seek insight into how companies' third-party service providers utilize artificial intelligence (AI) in each facet of the insurance product and delivery life cycle. They are asserting this through another vehicle, the proposed Exposure Draft of the Model Bulletin on the Use of Algorithms, Predictive Models, and Artificial Intelligence Systems by Insurers. The bulletin makes it clear that scrutiny of third parties will continue to build. The draft AI bulletin requires due diligence by the insurer to assess the third party when using its AI systems along with:[6]

- Requiring contract terms that entitle the insurer to audit the third-party vendor for compliance; the audits include confirming that the third party is complying with both contractual and regulatory requirements.
- Entitling the insurer to receive audit reports by qualified auditing entities to confirm compliance.
- Requiring the third party to cooperate with regulatory inquiries, investigations, and examinations related to the insurer's use of the third party's product or services.
- Including terms in contracts with third parties that require third-party data and model vendors and AI system developers to have and maintain AI system programs to the insurer's standards.

Stakeholder commentary

Industry and other groups, as well as some state regulators on the working group, urged the NAIC to hit the pause button and take time to get the model right amid a multitude of concerns of rushing the process. The reaction from industry and some regulatory stakeholders suggests that the adoption of the model will be delayed this year as the model is reworked.[7]

"We need more time to engage the public … it is too important a project to rush," said Katie Johnson, PPWG chair, on August 13 at the NAIC Summer National Meeting.

"This would not pass in Nebraska; it would not get past the front door," stated Martin Swanson, Nebraska Department of Insurance deputy director and general counsel, in a call the group hosted with industry and consumer advocates in late July.

"The Working Group has missed this opportunity to modernize and embrace steps taken by other regulators to meet the modern delivery demands and the sustainability expectations of consumers, where paperless digital delivery should be the default method unless the consumer requests the notice be mailed in hard copy format," stated the American Council of Life Insurers (ACLI) in a letter from July 28.[8]

"We should terminate the model," stated LeeAnn Crow, a Kansas regulator, telling fellow state regulators on the PPWG in a live meeting August 13 that the draft is fundamentally flawed and the opposition is multifaceted and would not pass in the Kansas state legislature.

"The working group is taking a novel approach to privacy, disregarding the structures insurers have been working under, and would replace it with something radically different. NAIC should pause and reflect and rewrite," stated Cate Paolino of the National Association of Mutual Insurance Companies (NAMIC) on the PPWG l July 25 call to discuss the model.[9]

"These issues are complex and we must recognize the necessary interplay with existing state and federal legal obligations as well as cross-sectional alignment within the model itself. As such, it is critical that the remainder of this process not be rushed," stated the American Property and Casualty Insurance Association (APCIA) in a letter dated July 28.[10]

Stakeholders additionally expressed concern that the language for joint marketing doesn't comport with the intent stated in the cover letter and needs to change to clearly allow joint marketing between financial institutions as authorized by the federal Gramm-Leach-Bliley Act (GLBA).[11]

"We all agree that these changes are long overdue, given that the previous NAIC models protecting consumer information were written decades ago, when abuses of consumer information were much less common," stated NAIC consumer representatives in a letter dated July 27.

Katie Johnson, chair of the working group and a Virginia insurance regulator, responded that she disagrees that the model is radical in its approach and stressed it protects consumers.

Key concerns expressed with the revised draft

Stakeholders in the industry said the draft, although changed from the earlier version to try to meet an initial barrage of concerns, is still too complex, lengthy, burdensome, and still has multiple disclosures with significant issues for the requirements for retention and deletion of data. Specifically, stakeholders voiced issues with the following:

- Security concerns based on consumer-available lists of all third-party service providers the insurer shares personal information with.
- Oversight of third-party service provider provisions are too broad and prescriptive, with unattainable requirements for vendors, such as the need to comply with each individual licensee's privacy practices, which can number in the thousands.
- Sharing limitations confined to permissible insurance transactions are problematic because activities related to insurance cannot be fully defined now or in the future, as business evolves. Any list would be too narrow as the market develops.[12]
- Joint marketing language is not clear enough to be practical and dovetail with established federal law (GLBA) and has unintended implications due to its language.
- Administrative obligations involving legacy systems and migration of data requirements are perceived as burdensome.
- The definitions of various components of the privacy process, including "additional activities," "consumer," and "biometric information."
- The model must be able to gain passage in state legislatures to deter federal oversight action.

Firms should be prepared if an updated draft model post-Version 1.2 gains traction

- Understand and implement a well-designed data governance program to build consumer trust and comply with upcoming regulatory scrutiny. This could include implementing upgraded policies for governing data, tools, and infrastructure to make certain that data inconsistencies in different systems across an organization are resolved, data is used properly, and data silos don't exist.
- Work closely with state insurance departments and the NAIC to get an idea of the scope of changes needed and what future exams might explore and target.
- Perform a risk assessment and review data management policies to identify areas that would require the most resources to adhere to the model law and areas that may present higher risk should the model gain traction. Work with relevant stakeholders of the firm to create an action plan.

Endnotes

1 National Association of Insurance Commissioners (NAIC), Privacy Protections (H) Working Group (PPWG), accessed August 2023; NAIC, Cover page for Draft Model Law #674 Version 1.2, July 11, 2023.

2 NAIC, NAIC Public Calendar, July 2023; NAIC, NAIC Consumer Representatives July 27, 2023 – Comments on Model 674 Exposure Draft, Version 1.2 (attach. 7 of PPWG), August 13, 2023; NAIC, Insured Retirement Institute (IRI) July 28, 2023 – Comments on Exposure Draft of New Insurance Consumer Privacy Protection Model Law #674 Version 1.2 (attach. 12 for PPWG), August 13, 2023.

3 NAIC, 2023 Summer National Meeting summary report for Innovation, Cybersecurity, and Technology (H) Committee, August 13, 2023.

4 NAIC, "2023 Privacy Protections (H) Working Group Workplan," July 10, 2023.

5 NAIC, NAIC Consumer Representatives July 27, 2023 – Comments (attach. 7 of PPWG), August 13, 2023.

6 NAIC, Exposure Draft 07.17.2023 – NAIC Model Bulletin: Use of Algorithms, Predictive Models, and Artificial Intelligence Systems by Insurers (attach. 3 of Innovation, Cybersecurity, and Technology (H) Committee), August 13, 2023.

7 NAIC, American Bankers Association (ABA) July 28, 2023 – Comments on Draft Insurance Consumer Privacy Protection Model Law #674 (attach. 13 of PPWG), August 13, 2023; NAIC, American Council of Life Insurers (ALCI) July 28, 2023 – Comments on Version 1.2 of the Draft Insurance Consumer Privacy Protection Model Law #674 (attach. 8 of PPWG), August 13, 2023; NAIC, National Association of Mutual Insurance Companies (NAMIC) – Comments on Consumer Privacy Protection Model Law #674 Version 1.2 (attach. 11 of PPWG), August 13, 2023; NAIC, American Property Casualty Insurance Association (APCIA) July 28, 2023 – Comments regarding July 2023 Draft of Consumer Privacy Protection Model Law #674 (attach. 10 of PPWG), August 13, 2023; NAIC, Reinsurance Association of America (RAA) July 27, 2023 – Comments regarding Exposure Draft of New Consumer Privacy Protection Model Law #674 (attach. 4 of PPWG), August 13, 2023; NAIC, Committee of Annuity Insurers (CAI) July 28, 2023 – Comments on Insurance Consumer Privacy Protection Draft Model Law #674 (attach. 14 of PPWG), July 28, 2023.

8 NAIC, ALCI July 28, 2023 – Comments (attach. 8 of PPWG), August 13, 2023.

9 NAIC, NAMIC July 28, 2023 – Comments (attach. 11 of PPWG), August 13, 2023.

10 NAIC, APCIA July 28, 2023 – Comments (attach. 10 of PPWG), August 13, 2023.

11 NAIC, ABA July 28, 2023 – Comments (attach. 13 of PPWG), August 13, 2023; NAIC, APCIA July 28, 2023 – Comments (attach. 10 of PPWG), August 13, 2023; NAIC, Independent Insurance Agents & Brokers of America (IIABA) July 24, 2023 – Comments regarding Draft Insurance Consumer Privacy Protection Model Law Version 1.2 (attach. 15 of PPWG), August 13, 2023.

12 NAIC, CAI July 28, 2023 – Comments (attach. 14 of PPWG), July 28, 2023.

Get in touch

Jordan Kuperschmid
Advisory Principal | Deloitte & Touche LLP
jkuperschmid@deloitte.com

Nitin Pandey
Advisory Managing Director | Deloitte & Touche LLP
napndey@deloitte.com

David Sherwood
Managing Director | Deloitte & Touche LLP
dsherwood@deloitte.com

Tim Cercelle
Managing Director | Deloitte & Touche LLP
tcercelle@deloitte.com

Deloitte Center for Regulatory Strategy

Irena Gecas-McCarthy
Principal | Deloitte & Touche LLP
igecasmccarthy@deloitte.com

Jim Eckenrode
Managing Director | Deloitte Services LP
jeckenrode@deloitte.com

Liz Festa
Senior Research Specialist | Deloitte Services LP
lfesta@deloitte.com

Contributors

Ashley Wells
Advisory Consultant | Deloitte & Touche LLP
aswells@deloitte.com

Rebecca Dangler
Advisory Analyst | Deloitte & Touche LLP
rdangler@deloitte.com

8

Center *for*
Regulatory Strategy US

About the Center
The Deloitte Center for Regulatory Strategy provides valuable insight to help organizations in the financial services industry keep abreast of emerging regulatory and compliance requirements, regulatory implementation leading practices, and other regulatory trends. Home to a team of experienced executives, former regulators, and Deloitte professionals with extensive experience solving complex regulatory issues, the Center exists to bring relevant information and specialized perspectives to our clients through a range of media, including thought leadership, research, forums, webcasts, and events.

Deloitte.