



J. Kevin A. McKechnie  
Senior Vice President  
Office of Insurance Advocacy  
kmckechn@aba.com

April 3, 2023

Ms. Katie Johnson  
Virginia State Corporation Commission/Bureau of Insurance  
Chair, NAIC Privacy Protections Working Group  
NAIC Central Office  
1100 Walnut Street, Suite 1500  
Kansas City, MO. 64106

Attn: Ms. Lois Alexander, NAIC Market Regulation Manager  
Sent via email: [lalexander@naic.org](mailto:lalexander@naic.org)

**RE: Draft Insurance Consumer Privacy Protection Model Law #674 –  
Comments of the American Bankers Association’s Office of Insurance  
Advocacy**

Dear Ms. Johnson:

Thank you for the opportunity to offer comments to the exposure draft of proposed Model Law #674 (the “Exposure Draft”). The American Bankers Association (“ABA”) is a longtime supporter of, and collaborator with, the National Association of Insurance Commissioners (“NAIC”). We appreciate being considered an interested party to the Privacy Protection Working Group’s (“PPWG”) drafting process and we intend to remain a part of that process until its conclusion.

While we support the Working Group’s efforts to unify and modernize Model Law #670 and Model Regulation #672, if implemented in its current form, the Exposure Draft conflicts with federal privacy laws and would hurt the very consumers it aims to protect. The ABA writes to ask the Working Group to revise the Exposure Draft to either provide an exception to its requirements for financial institutions and their affiliates that are already subject to the Gramm-Leach-Bliley Act (“GLBA”) or alternatively, ensure that it does not conflict with or unnecessarily duplicate federal privacy laws.

The importance of protecting consumer data and privacy are not new concepts for ABA member banks and their insurance affiliates. For over two decades, banks have been required to comply with the GLBA and its implementing regulations.<sup>1</sup> As noted by President Clinton, the GLBA protects consumers by requiring banks to:

[C]learly disclose their privacy policies to customers up front...consumers will have an absolute right to know if their financial institution intends to share or sell their personal financial data, either within the corporate family

---

<sup>1</sup> 15 U.S.C. §§ 6800 et seq. and implementing regulations.

or with an unaffiliated third-party [and]...will have the right to 'opt out' of such information sharing with unaffiliated third parties...[and] allows privacy protection to be included in regular bank examinations...[and] grants regulators full authority to issue privacy rules and to use the full range of their enforcement powers in case of violations.<sup>2</sup>

Model Regulation #672 was based on the GLBA and despite the Exposure Draft purporting to merely update and improve Model Regulation #672, the Exposure Draft represents a significant departure from longstanding privacy practices that banks and consumers have become accustomed to.

Several key provisions from Model Regulation #672 were not included in the Exposure Draft. For example, Section 15 of Model Regulation #672 (titled "Exception to Opt-Out Requirements for Disclosure of Nonpublic Personal Information for Services Providers and Joint Marketing") is absent from the Exposure Draft. The exception language found in Section 15 (commonly known as the "service provider/joint marketing exception") mirrors language from the GLBA's privacy provisions. The exception permits financial institutions to disclose a consumers' nonpublic information to nonaffiliated third parties for marketing purposes without first having to give consumers the right to opt-out of the information sharing. The joint marketing exception benefits consumers by helping them more readily access a wider variety of financial services and insurance products, reducing insurance costs, and providing consumers with increased conveniences.

While we are supporters of a state-based approach to insurance regulation, we believe the Exposure Draft's elimination of the joint marketing exception is preempted by the GLBA. The GLBA preempts state privacy laws to the extent that compliance with a state law would be "inconsistent with" the requirements of the GLBA.<sup>3</sup> Moreover, under the GLBA:

[N]o State may, by statute, regulation, order, interpretation, or other action, *prevent or significantly interfere* with the ability of a depository institution, or an affiliate thereof, to engage, directly or indirectly, either by itself or in conjunction with an affiliate or any other person, in any insurance sales, solicitation, or *cross-marketing activity*.<sup>4</sup> (Emphasis added)

We have concerns that other provisions in the Exposure Draft may also be inconsistent with the requirements of the GLBA and thus preempted. For these reasons, we believe the Working Group should revise the Exposure Draft to provide an exemption for financial institutions and their affiliates that are already subject to the GLBA. Several states have recently taken this exact approach in enacting privacy legislation. For example, Colorado's privacy law expressly exempts a "financial institution or an affiliate

---

<sup>2</sup> William J. Clinton, Statement on Signing the Gramm-Leach-Bliley Act, November 1999, <https://web.archive.org/web/20160322081604/http://www.presidency.ucsb.edu/ws/?pid=56922> accessed April 3, 2023.

<sup>3</sup> 15 U.S.C. § 6807(a).

<sup>4</sup> 15 U.S.C. § 6701(d)(2)(A).

of a financial institution” that is subject to the GLBA.<sup>5</sup> Virginia’s privacy laws similarly exempt a “financial institution or data subject to Title V of the federal Gramm-Leach-Bliley Act.”<sup>6</sup>

The preemption issue is also relevant to ongoing efforts to modernize and enhance federal privacy laws under the GLBA. For example, Rep. Patrick McHenry (R-NC), Chair of the House Financial Services Committee, has introduced the Data Privacy Act of 2023 (H.R. 1165), which would amend the GLBA to expressly provide for a uniform privacy regimen that would preempt all state privacy laws.

We bring these issues to you so the lack of a GLBA exemption does not impede your work as a whole. We have every confidence the Working Group will be cognizant of the unique federal privacy laws banks and their insurance affiliates are already subject to and look forward to being part of the comment process as the NAIC works to modernize its model privacy laws.

Respectfully,

A handwritten signature in black ink that reads "J. Kevin A. McKechnie". The signature is written in a cursive style with a large initial "J" and "K".

J. Kevin A. McKechnie  
Senior Vice President  
American Bankers Association  
Office of Insurance Advocacy

---

<sup>5</sup> Colo. Rev. Stat. § 6-1-1304(2)(q).

<sup>6</sup> Va. Code Ann. § 59.1-576(b)(ii).

April 3, 2023

Katie Johnson, Chair  
Privacy Protections (H) Working Group  
National Association of Insurance Commissioners  
1100 Walnut Street, Suite 1500  
Kansas City, MO 64106-2197

*Attn: Lois Alexander, NAIC Market Regulation Manager*  
Via email: [lalexander@naic.org](mailto:lalexander@naic.org)

**RE: ACLI Comments on the Draft Insurance Consumer Privacy Protection Model Law (#674)**

Dear Chair Johnson:

Thank you for the opportunity to provide comments on the Insurance Consumer Privacy Protection Model Law (#674) and for the addition of biweekly open calls and an in-person stakeholder meeting. We appreciate the time, energy, and consideration already undertaken by members of the Working Group and look forward to continued conversations as the necessary improvements begin to take shape.

ACLI members believe Model #674 must be carefully crafted to strike a balance between protecting consumer privacy and enabling insurers to meet the needs of their customers effectively. At a high level, these comments are meant to highlight several provisions ACLI members find troubling in the initial exposure draft. Key areas of concern include the provisions relating to prior consent for marketing; prior consent for actuarial studies and research studies; limitations on collection, use, and sharing of personal information to insurance transactions; prior consent for overseas processing; 90 day deletion and privacy notice obligations; overly-prescriptive notice and consent requirements; oversight of third-party service providers; response times for access and correction; the optional private cause of action; and definitional concerns. We hope these initial comments provide some background on how and why life insurers use personal information, helpful context on how the identified provisions may negatively impact business operations, and some constructive recommendations on how to begin addressing industry concerns.

Important Considerations- How and Why Life Insurers Use Personal Information

ACLI member companies believe consumers and companies need consistent privacy rules providing equal protections across the country. A patchwork quilt of differing state-by-state or sector-specific

**American Council of Life Insurers** | 101 Constitution Ave, NW, Suite 700 | Washington, DC 20001-2133

---

The American Council of Life Insurers (ACLI) is the leading trade association driving public policy and advocacy on behalf of the life insurance industry. 90 million American families rely on the life insurance industry for financial protection and retirement security. ACLI's member companies are dedicated to protecting consumers' financial wellbeing through life insurance, annuities, retirement plans, long-term care insurance, disability income insurance, reinsurance, and dental, vision and other supplemental benefits. ACLI's 280 member companies represent 94 percent of industry assets in the United States.

privacy regulations is confusing, frustrating, and not helpful to consumers. While modernization of existing privacy laws should be considered as advances in technology support collection and analysis of an ever-increasing amount of personal data, we believe regulatory proposals that would increase complexity must be avoided (e.g., consumer rights that would differ across states, require varying levels of protections, or create fragmented implementation and legal uncertainty).

Insurers are required to conform to an overlapping mix of longstanding and evolving federal and state privacy laws and regulations. These existing laws continue to enable an essential balance between consumers' growing demand for convenience and personalized service and their valid privacy concerns about the collection, use, and sharing of their personal information. Additionally, insurers spend millions of dollars annually to maintain cybersecurity and comprehensive information security programs to appropriately safeguard the personal information entrusted to them.

The fundamental nature of the business of insurance requires carriers to collect highly sensitive personal information for the purpose of evaluating risks and we believe it is important for insurance regulators to distinguish our industry from other businesses in the data driven technology sector. Unlike industries where consumer data is viewed as a product to be monetized, insurers use personal information to meet customer needs, ultimately providing protection for individuals and their families. Insurers are not Big Tech. In comparison to recent scandals and controversies involving technology companies and platforms, there are relatively very few complaints about insurers privacy practices, or findings in published market conduct examination reports that suggest that insurers, or their service providers are misusing the personal information of consumers and customers that they collect. While there is room to improve the existing regulatory structure, existing rights and obligations regarding collection, processing and sharing should not be changed in ways that may conflict with regulations enacted pursuant to GLBA or the pre-emptive affiliate sharing provisions of FCRA or should be confined to very narrowly defined insurance transactions that could compromise insurers' ability to meet the needs, expectations, and desires of their customers most effectively.

### Initial Concerns

Below we highlight a few provisions that need to be discussed in more detail, as we foresee potentially negative consequences. We have included tentative suggestions for edits to these provisions that we hope you find constructive and helpful. Our members have also identified a number of more discrete concerns with other provisions in the Model, but many of those concerns are interrelated with the concepts raised below. We believe ACLI members will be better able to offer recommendations on these provisions after the Working Group has shared additional context around their purpose and intent, and look forward to doing so during upcoming open calls and the in person drafting session. Please know that for each provision we are thoughtfully considering how best to balance the intent of the Working Group with legitimate business practices.

While the ACLI has worked in good faith to flag potential issues and offer constructive suggestions, our comments here are preliminary and subject to change based on how the intent behind certain provisions is made clearer and the draft continues to take shape. As the draft Model language continues to evolve, we request sufficient time to revisit these concerns and recommendations. Please consider these ACLI's initial primary concerns with more comments to come.

## 1. Prior Consent for Marketing

ACLI members are concerned by the requirement that licensees obtain a consumer's consent before using a consumer's personal information to market a product or service to the consumer, even if the consumer is an existing customer, as well as the resulting prohibition on joint marketing with trusted financial institutions. This would be an extreme requirement that goes beyond any of the general state privacy laws – and one that would have real impacts on the sale of life insurance, particularly in underserved markets. Life insurers are in the industry of providing products to customers to help them financially, and if not able to properly market to their own pool of customers, there are likely to be missed opportunities and potential distress to customers not being made aware of their full suite of financial products/options. Marketing increases consumers' awareness of financial risks and ways to address them.

At a time when industry and regulators are focused on closing the coverage gap and building financial resilience, the draft language will deny millions of existing customers, as well as new consumers, the opportunity to learn about products, services, and upgrades that may benefit them and their families. For example, this would unnecessarily prohibit joint marketing with trusted financial institutions and result in less valuable, more expensive, and less convenient insurance products and/or services for consumers, especially middle-market and underserved consumers. At an industry level, we would expect increased costs as insurance companies and producers are forced to turn to less efficient forms of marketing. This will hurt mid-size and small licensees more, and most importantly will make insurance products less available to consumers, especially the consumers in underserved populations.

**Tentative Suggestion(s)-** Consider clarifying definitions and exemptions. Consider amending to “opt out.” Current privacy laws applicable to financial institutions balance consumer control with a company's need to collect and share information for normal business practices. These laws include, but are not limited to, the Gramm-Leach Bliley Act (GLBA), the NAIC Privacy of Consumer and Health Information Regulation (Model #672), and Fair Credit Reporting Act (“FCRA”). They provide examples of adequate notice as well as reasonable opt-out means, including an electronic opt-out option. The existing NAIC Models include a set of exemptions for business functions that preserve a licensee's ability to share information to conduct the business of insurance. Model #672 does not restrict any disclosure of nonpublic personal information with affiliates and allows licensees to share nonpublic personal financial information with unaffiliated financial institutions subject to a joint marketing agreement. Many states with Model #670 have revised their law to incorporate a joint marketing exception and to remove the limits on disclosures to affiliates. While updates may be warranted for new technologies, we believe that the balanced opt-out approach remains appropriate and effective to respect consumers' privacy preferences. ACLI members are considering additional recommendations and look forward to thoughtful engagement with the Working Group during upcoming open calls and the in person drafting session.

## 2. Prior Consent for Actuarial Studies and Research Studies

ACLI members appreciate the fact that actuarial or research studies for rating or risk management purposes of the licensee are covered by the definition of “insurance transaction.” Therefore, as the Model is constructed, it is not necessary to obtain consumer consent to use personal information for these purposes. However, requiring a consumer opt-in for any “research activities not related to rating or risk management for or on the behalf of the licensee” creates confusion and hampers insurers' ability to conduct meaningful research. Data analysis of any kind depends on having a valid

statistical dataset; and if opt-outs are not perfectly random across the dataset they will skew the data and make it meaningless. Insurance licensees would be limited in their ability to conduct internal research, certain risk analysis, and measure customer satisfaction. Insurers will potentially not be able to test out new underwriting data sources, build accelerated underwriting models, monitor customer experience, or conduct research studies to improve products and processes. Insurers do not need to disclose personal information in reports or studies, but they need the data to be available to conduct the studies. This will also substantially limit and hinder insurer's ability to provide meaningful experience analysis. Experience studies and monitoring are currently used to effectively understand and manage the business; for valuation to support IFRS and NAIC reserve assumptions; and could impact NAIC cashflow testing and reserve requirements. For reinsurers, there is an added layer of concern because without having a direct contractual relationship with the insured, it would be difficult to ever obtain consent for critical research or experience studies.

**Tentative Suggestion(s)-** Consider clarifying through the addition of a definition for “research studies and the addition of exemptions in certain circumstances. Consider organizing the Model so the exceptions are all in one section (and then indicating which ones correspond to notice, opt-in/out, and the various requests). ACLI members are considering additional recommendations and look forward to thoughtful engagement with the Working Group during upcoming open calls and the in person drafting session.

### 3. Limitations on Collection, Use, and Sharing of Personal Information to Insurance Transactions

ACLI members are concerned that the prohibition in Section 4(A) on collection, processing, retaining, and sharing consumer's personal information unless it is “in connection with an insurance transaction as defined in this Act” will have unintended consequences for companies' non-insurance products and services. This concern is rooted in the conflict between the broad application to and definition of “licensees” versus the tailored definition of “consumer.” If licensees are prohibited from collecting any individual's personal information unless tied to an insurance transaction, many non-insurance products and services will grind to a halt. For instance, many companies and their affiliates offer not only insurance products, but also planning, securities brokerage, and investment advisory products and services to best meet their clients' needs in a more holistic manner. This is consistent with the existing regulatory structure created by the combination of GLBA and FCRA. Importantly, securities recommendations must be reviewed and supervised by a FINRA-licensed entity, irrespective of whether the recommendation relates to an insurance transaction. Also, to offer planning, insurance, securities brokerage, and investment advisory products and services, advisors should typically be aware of a client's entire financial situation, including their insurance and investment holdings. Because the proposed limitations on collection, use, and affiliate sharing do not appear to accommodate purposes beyond “insurance transactions,” they would put these comprehensive approaches to financial security at risk for consumers. In addition, affiliates of licensees that do not engage in insurance transactions essentially would be barred from sharing technology systems with licensees for fear of running afoul of that limitation.

**Tentative Suggestion(s)-** The NAIC should not impose barriers to companies offering this type of important financial security to their customers. A helpful resource explaining why the current approach to data minimization will harm not just companies, but their customers as well, is EY's recent published research regarding maximizing retirement outcomes by allocating assets at the global level between equities, bonds, and fixed income. EY's evaluation presupposes an insurer/advisor's ability to share information with its broker-dealer arm to help clients achieve better outcomes. (See [How insurance and investments can improve financial wellness | EY - US](#)). ACLI

members are considering additional recommendations and look forward to thoughtful engagement with the Working Group during upcoming open calls and the in person drafting session.

#### 4. Prior Consent for Overseas Processing

ACLI members are concerned with the prohibition on collecting, processing, or maintaining personal information outside the United States without a consumer's consent, severely limiting the ability to use offshore affiliates and service providers. There would be significant operational impact on companies because it would prevent them from engaging service providers located outside the U.S. or even U.S.-based service providers that have data centers or data processing activities outside the United States. For companies who engaged in global operations, this new requirement would have a heightened impact insofar as it would apply even to intracompany data transfers and data processing activities. If an international insurer has operations in Germany and the U.S., the U.S. operation could not transfer data to Germany for any processing activity, even if security in Germany is equivalent or better than the U.S. This would decrease efficiency in many areas (infrastructure, resources, personnel), thereby adding costs and not serving the consumer. For global reinsurers, this would be significantly challenging in that it would restrict their ability to manage data within their own companies. Further, as drafted, the limitation on transferring information outside of the United States is contrary to the free flow of data and prohibition on data localization policy positions and commitments adopted by the U.S. in its trade agreements, at the G7, and in its financial regulatory dialogues. The limitation is not only inconsistent with U.S. policy positions, but also contrary to the positions adopted by U.S. peer countries such as the EU, UK, Singapore, Japan, and Australia. These governments support the free flow of data, including for personal information, and the need to prohibit data localization requirements while at the same time maintaining privacy frameworks. The European Union's General Data Protection Regulation (GDPR) does not impose a prior express consent basis for the overseas transfer or processing of personal information. Singapore, Australia, Japan, and the United Kingdom maintain privacy frameworks without restricting the free flow of data outside their territories. These countries, like the United States, also have entered into free trade agreements that include commitments to the free flow of data and prohibition on data localization. Ultimately, many data privacy and security concerns are already addressed under the NAIC Insurance Data Security Law (Model #668), the GLBA Safeguards Rule as adopted by states, and other regulatory frameworks to which insurers are subject. Additional concerns can be addressed through contractual obligations.

**Tentative Suggestion(s)-** ACLI members believe it is more appropriate to address security concerns through due diligence and contractual obligations. Functionally, these service relationships are already subject to a number of restrictions, including contractual certifications on use/access, cybersecurity oversight, etc. ACLI members are considering additional recommendations and look forward to thoughtful engagement with the Working Group during upcoming open calls and the in person drafting session.

#### 5. 90 Day Deletion and Privacy Notice Obligations

ACLI members are also concerned with the requirement to delete consumer personal information if it is no longer necessary to perform specific "permitted purposes" after 90 days and to provide notice to consumers regarding the deletion from both insurer and all third-party service providers. Personal data that is no longer necessary for a permitted purpose should be securely deleted or disposed of in accordance with applicable laws and regulations. Insurers have many policies and procedures in place to ensure that personal data is only retained for as long as necessary and that it is securely



disposed of when it is no longer needed. However, the 90-day deletion period included in the draft Model is unworkable. Many legacy systems that hold customer data are not designed to be able to do purging, automatic, or otherwise. Additionally, the new obligation in Section 5(B)(3) to send a privacy notice after deletion goes against the overall trend in state adoption of the 2015 FAST Act amendment to the GLBA and general privacy models to decrease the frequency of delivering privacy notices and/or to allow for provision of notice via a website or other electronic means. Given that several service providers may touch customer data, confirming deletion on a customer-by-customer basis would be unmanageable.

**Tentative Suggestion(s)-** Consider a “reasonable period of time,” rather than 90 days, as well as the adoption of a feasibility standard similar to the one included in the New York Department of Financial Services’ Part 500. ACLI members are considering additional recommendations and look forward to thoughtful engagement with the Working Group during upcoming open calls and the in person drafting session.

## 6. Overly Prescriptive Notice and Consent

ACLI members are concerned with the overly prescriptive notice (Section 8) and consent (Section 9). It is critical to avoid crafting a new Model that would impede innovation in the insurance industry and undermine longstanding business and actuarial practices. An overly prescriptive Model may also hamper uniform adoption by the states, thereby undermining one of the Working Group’s key objectives. Additionally, the expansion of notice obligations (Section 6) to include beneficiaries, would affect long-standing rules around how life insurers treat beneficiaries prior to time of claim. It presents some practical concerns, as someone receiving a privacy notice might request an explanation of why they are receiving the privacy notice. Beneficiary designations can and do change over the lifetime of a policy – and this requirement might inadvertently require life insurers to reveal an insured’s estate plans before they are ready to do so. This would be especially problematic in the case of contingent beneficiaries. It would also impact long-standing practices around administration of group insurance business. For some group products, insurers might not know the identities of all the certificate holders or have their mailing addresses. This sets up a system where they would be required to collect additional personal information to comply with the Model. Further, it would also impact reinsurers, as they typically do not collect information from a consumer and have no direct interaction with them. Reinsurer notice obligations would be confusing and counterproductive. Ultimately, some of these changes would increase complexity, cost, and the number of notices individuals receive, all at a time when the trend is to decrease the frequency of notices or provide them by alternative means.

### **Tentative Suggestion(s)-**

- Instead of providing notice prior to collecting personal information, consider requiring insurers to provide initial notice within a reasonable amount of time after collecting personal information.
- Consider paperless digital delivery and/or website posting as the default method unless the consumer requests otherwise.
- Provide an exemption for reinsurers, consistent with the breach notice requirements under other privacy protection schemes, such as the NAIC Insurance Data Security Model Act (#668) and NYDFS Part 500.
- Reconsider the inclusion of “beneficiaries” for notice obligations.
- Consider making it clear that an insurer can continue to satisfy the requirement through delivery of a privacy notice to the group policyholder in lieu of delivery to each insured under

the group policy. Consider using existing language from the Privacy of Consumer Financial and Health Information Regulation (Model #672) Section 10, “*Unless a licensee is providing privacy notices directly to covered individuals described in [Section 4F(2)(e)(i), (ii) or (iii)], a licensee shall provide initial, annual and revised notices to the plan sponsor, group or blanket insurance policyholder or group annuity contract holder, or workers’ compensation policyholder, in the manner described in Sections [5 through 9] of this [regulation], describing the licensee’s privacy practices with respect to nonpublic personal information about individuals covered under the policies, contracts or plans.*”

- ACLI members are considering additional recommendations and look forward to thoughtful engagement with the Working Group during upcoming open calls and the in person drafting session.

## 7. Oversight of Third-Party Service Providers

ACLI members are concerned by the additional provisions relating to the oversight of third-party service providers, given existing requirements in the Insurance Data Security Law (Model #668) and the GLBA Safeguards Rule as adopted by states, and other regulatory frameworks to which insurers are also subject. Insurers already impose contractual restrictions on their third-party service providers requiring them to process data only for the purpose of providing services (with limited exceptions for legal obligations, cybersecurity measures, etc.), restricting them from sharing the data with additional parties without contractual protections in place, and prohibiting them from retaining the data longer than required to provide the services. As written, the draft appears to require licensees to conduct extensive diligence on all third-party service providers and to enter into a written agreement that requires each third-party to comply with both the Model #674 requirements and the licensee’s own practices in connection with the collection and use of consumers’ personal information. It would be extremely onerous, if not impossible, for most third-party service providers to comply with each of their insurer clients’ practices in addition to the significant limitations already imposed upon their use, sharing, and retention of insurer data. Having this extensive and restrictive contractual requirement apply to all third-party service providers would be burdensome for licensees to negotiate service provider agreements with third parties in practice. Insurers may be forced to contract with smaller vendors that often have weaker cybersecurity protections and will be less capable of responding to individual rights requests. The net effect of this provision will weaken the cybersecurity and privacy protections afforded to consumers. Furthermore, many insurers will be subject to multiple state versions of the model law. Third-party service providers will therefore have to contractually agree to comply with numerous state laws they have no experience complying with.

**Tentative Suggestion(s)-** Consider a less restrictive approach. For instance, U.S. state and foreign privacy laws take a more reasonable approach, where third-party service providers are contractually required to process data only for the purpose of providing services (with limited exceptions for legal requirements, cybersecurity measures, etc.), restricted from sharing the data with additional parties without contractual protections in place, and prohibited from retaining the data longer than required to provide the services. ACLI members are considering additional recommendations and look forward to thoughtful engagement with the Working Group during upcoming open calls and the in person drafting session.

## 8. Response Times for Access and Correction

ACLI members are also concerned with the response times for access and correction. Many of the included response times are significantly shorter than Model #670, HIPAA, and what is required by

state laws such as the CCPA/CPRA. Operationally, it would be very challenging for insurers to comply with these reduced time frames, which would provide little benefit for consumers. Insurers often process large volumes of data, which can make it challenging to respond quickly to these types of requests. It takes time to retrieve and review the relevant data before responding to a request, especially if it is complex. Insurers must also verify a customer's identity before providing access to or making corrections to their personal data. New limitations, such as these extremely short response times, will have significant financial impacts on our companies, our consumers, and our partners.

**Tentative Suggestion(s)-** The five-day acknowledgement period should be synchronized with the CCPA (10 business days) to make the requirement more manageable. The 15-day response times should be changed to 45 days to mirror the CCPA and match the existing standard. Include an option for additional 45-day extension in certain circumstances to match CCPA. The request should not be considered “received” until the licensee has been able to verify the consumer’s identity. ACLI members are considering additional recommendations and look forward to thoughtful engagement with the Working Group during upcoming open calls and the in person drafting session.

#### 9. Optional Private Cause of Action

ACLI members are opposed to the inclusion of an optional private cause of action. Insurers support strong consumer protections governing the creation, distribution, and administration of all life insurance products. State insurance regulators have a wide variety of tools at their disposal to enforce insurance laws and regulations. Every state has enacted the NAIC Uniform Unfair Trade Practices Act, which includes an escalating ladder of remedies for a wide array of wrongful conduct. These remedies include monetary penalties, cease and desist orders, mandatory hearings, and discovery, and even license suspension and revocation. These enforcement mechanisms are sufficient to protect consumers.

**Tentative Suggestion(s)-** ACLI members oppose the inclusion of an optional private cause of action.

#### 10. Definitions

ACLI members have several concerns with the definitions in Section 3, with many of those concerns being interrelated with the concepts raised above. Below we highlight a few definitions that need to be discussed in more detail, as we foresee potentially negative consequences. This list is not all encompassing, and additional issues impacting definitions will need to be discussed during the open calls and in person meeting. We also believe ACLI members will be better able to offer recommendations on these definitions after the Working Group has shared additional context around their purpose and intent, and additional drafting is completed.

Certain definitions are overly-broad. For instance, the definition of “Insurance Support Organization,” as written, would capture nearly any company that works with an insurer. The definition of “Share, Shared, or Sharing” would apply to all the disclosures insurers currently may engage in with third-party service providers, vendors, etc., for core administrative purposes that allow them to service existing business and process claims efficiently and affordably to the benefit of customers. Another example is the expanded definition of “Consumer,” which has implications for several of the other concerns identified above and may create conflicts with policies issued in states that have adopted the NAIC Value Added Services Model.

Other definitions, as written, are too narrow. For example, the definition of “Insurance Transaction” seems to ignore financial institutions that have financial products outside of insurance. It also ignores member-based organizations where membership creates a customer relationship and data is shared but no insurance product is purchased. The definition of “Value-Added Service or Benefit” ignores financial institutions that offer a variety of financial products, including insurance, and does not line up with the new definition under the NAIC Unfair Trade Practices Act.

Additionally, some terms used throughout the draft Model are not currently defined, which contributes to some confusion around related provisions. For instance, the terms “Actuarial Studies” and “Research Studies.”

Finally, several definitions, including “Insurers”, “Licensees”, and “Third-Party Service Providers” are also unclear in so far as to whether, and to what extent, reinsurers or producers are included in the applicable definitions. As a result, it is not clear how the law would apply to reinsurers or producers, and what their obligations are under it.


**Tentative suggestion(s):** Revisit the Definitions section after additional drafting is complete. Consider aligning certain definitions to the approach used in existing NAIC Models or state privacy laws. An unnecessary disparity in definitions opens the door to confusion and a lack of harmony between regulatory expectations. Amend the definitions to clarify its scope and application to reinsurers and producers. ACLI members are considering additional recommendations and look forward to thoughtful engagement with the Working Group during upcoming open calls and the in person drafting session.

## Conclusion

ACLI is proud of our member companies’ longstanding role as conscientious and responsible guardians of consumers’ personal information. We remain strongly committed to the proper use and protection of personal information. We reiterate our appreciation of the additional opportunities for open meetings- both in-person and remote- which will provide a meaningful forum for regulators to thoughtfully engage with industry and consumer representatives during the drafting process. ACLI looks forward to collaborating with the Working Group throughout the drafting process and providing additional constructive recommendations in the coming months.

Thank you for your consideration of our comments. We welcome any questions.

Sincerely,



Kristin Abbott

*Counsel*

American Council of Life Insurers



April 3, 2023

Katie Johnson, Chair  
Privacy Protections (D) Working Group  
National Association of Insurance Commissioners  
1100 Walnut Street, Suite 1500  
Kansas City, MO 64106-2197

By Email to Lois Alexander at [LAlexander@NAIC.org](mailto:LAlexander@NAIC.org)

**Re: Draft Consumer Privacy Protections Model Law #674 – AHIP Comments**

Dear Ms. Johnson:

On behalf of the members of AHIP, we appreciate the opportunity to provide comments on the Draft of the proposed Consumer Privacy Protections Model Law #674. We ask you to view these comments much as you view the Draft Model itself – as a work in progress. As we work together on the Model, we expect both the Model and some of our views to be refined and narrowed as we go, as regulators, consumer groups, and industry exchange views on the competing policy goals and practical applications of this proposal.

**Work Plan and AHIP’s Approach.**

As a foundational matter, AHIP members applaud the newly released workplan schedule for its recognition of the daunting breadth of this effort, and the realization that the most effective and efficient way forward is a series of discussions among all parties on a regularly scheduled basis. This procedure will advance the overall knowledge base of all participants, a critical element of developing any model in such a highly technical, complex, and rapidly evolving field as privacy.

We also believe that multiple provisions of the Draft Model which present relatively clear-cut policy questions can be easily remedied without sacrificing the core policy goals of the Model. As such, these “low-hanging fruit” can and should be addressed early in these efforts, in order to shorten the draft and allow all parties to focus on more complex topics. In the interest of avoiding a lengthy comment letter, we are limiting ourselves to these straightforward issues.

**Section 19: The HIPAA Safe Harbor.** As we have stated repeatedly since the beginning of this effort over two years ago, most of AHIP’s members are subject to the requirements of the Health Insurance Portability and Accountability Act (HIPAA); the Privacy and Security Rules

promulgated under HIPAA (45 C.F.R. Parts 160, 164); the Health Information Technology for Economic and Clinical Health (“HITECH”) Act (Pub. L. No. 111-5) and regulatory changes made pursuant to HITECH; and the 2020 Interoperability and Patient Access Final Rule (85 FR 25510) (“Interoperability Rule”). This legal framework tightly restricts an insurer’s use and handling of an individual’s protected health information (PHI) and imposes parameters on permitted uses and disclosures for essential functions such as payment, treatment, and healthcare operations. The Privacy Rule provides consumers with broad rights related to their health information, including the right to request correction or amendment of incorrect information, data portability, and the right to request restrictions or disclosures of their information.

Although Section 19 of the Draft Model law provides a “deemed compliance” Safe Harbor for entities that have to comply with HIPAA and HITECH (hereafter, “HIPAA” for simplicity), it only provides partial exemption from other model law requirements and still imposes other requirements for licensees that HIPAA’s protections already cover. We outline those below, and provide a link to the full HIPAA Administrative, Privacy, and Security Rules to supply the primary source of the requirements for more details, below on page 3.

**Model #674, Section 2. Oversight of Third-Party Service Provider Arrangements.**

The comparable provisions of the HIPAA Rules, 45 CFR 164.308(b)(1)-(3), allow sharing of PHI only if the Covered Entity receives contractual assurances from the “Business Associates” as required by 45 CFR 164.314(a) to the Covered Entity. These assurances generally require the Business Associate to abide by all the same restrictions and provisions required of the Covered Entity under the HIPAA Privacy and Security Rules. Additionally, the contract between the Covered Entity and the Business Associate (the “Business Associate Agreement”) must meet the requirements set out in 45 CFR 164.504(e)(1). Unlike the NAIC Draft Model, HIPAA’s HITECH amendments also provide equal jurisdiction to enforce HIPAA/HITECH on the Business Associate and Covered Entities. For additional information, see <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html>

**Model #674, Section 9. Consumers’ Consent – How Obtained.** HIPAA’s Privacy Rule generally limits Covered Entities’ uses and disclosures of PHI without individual’s express authorization to those necessary to support treatment, payment, or health care operations (45 CFR 164.506), or to those uses and disclosures set out in detail in 45 CFR 164.512, such as required by (a) law; (b) for judicial and administrative proceedings; (c) for public health activities or health oversight activities; (d) for law enforcement; (e) for certain research purposes; as well as (f) limited disclosures about victims of abuse, neglect, or domestic violence, and other similar specifically enumerated purposes.

**Model #674, Section 10. Content of Authorizations.** The HIPAA Rules’ detailed requirements for a valid authorization by an individual to disclosure of his or her PHI are in 45 CFR 164.508(b) and (c).

**Model #674, Section 11. Access to Personal Information.** Under the HIPAA Privacy and Security Rules, an individual’s right to access their own PHI is detailed in 45 CFR 164.524.

**Model #674, Section 12, Correction or Amendment of Personal Information.** Under the HIPAA Privacy Rules, an individual’s right to correct or amend their PHI is set out in detail in 45 CFR 164.526.

**Model #674, Section 13, Nondiscrimination and Nonretaliation.** The HIPAA Privacy and Security Rules specifically state a Covered Entity or Business Associate may not threaten, intimidate, coerce, harass, *discriminate* against, or *take any other retaliatory action* against any individual or other person for, among other things, opposing any act or practice made unlawful by this subchapter (emphasis added). See 45 CFR 160.316.

To locate and review the specific HIPAA citations, the complete HIPAA Administrative Simplification Rules are here: <https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf>. This publication includes not only the complete HIPAA Privacy and Security Rules, but also other administrative requirements for the use and contents of the uniform electronic claims and payment operations system for standard transactions which is used by health insurers, providers, and government payors throughout the country. As these are reviewed by regulators, we’d note that the HIPAA/HITECH requirements substantially meet the apparent purposes and policy goals of the Draft Model #674. In most cases, the HIPAA requirements are more extensive and detailed, as these requirements were carefully calibrated to balance privacy rights and responsibilities, and make sense in the unique context of healthcare, through years of comments and rulemaking among the relevant stakeholders. Therefore, it must be recognized that any effort to require health insurers to vary from the national HIPAA requirements in those states which ultimately enact the proposed NAIC Model would serve only to defeat the efficiency and cost-savings which result from HIPAA’s uniform application throughout the American health care system.

**Model #674, Section 19: The HIPAA Safe Harbor – “Additional Permitted Transactions.”** Section 19.A(1)(a) of the Draft Model raises other concerns. It would require a consumer’s consent before a licensee engaged in any “additional permitted transactions.” As defined in Section 3.B., additional permitted transactions would include using a consumer’s information for (1) marketing purposes and (2) certain research purposes. The second use case is the most concerning since it conflicts with existing HIPAA language. The HIPAA Privacy Rule provides a Covered Entity need not seek individual authorization to use or disclose Protected Health Information for research purposes if it *has been de-identified* (in accordance with 45 CFR 164.502(d), and 164.514(a)-(c)(emphasis added). The HIPAA Privacy Rule also allows the use and disclosure of PHI for research purposes, subject to compliance with a series of conditions and requirements to limit the use of PHI to the minimum necessary to support the research. More details on these protections, too extensive to be set out in this letter, are available at this HHS link: <https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html>.

**Model #674, Section 19: The HIPAA Safe Harbor – Sharing Outside the U.S.** Also concerning is language in Section 19.A(1)(b) which limits the sharing of a consumer’s information outside the jurisdiction of the United States or its territories. Most if not all insurers already share or store data outside the United States, and often use offshore customer service and other third-party vendor services. This privacy of consumer information is already well addressed in HIPAA in its Privacy Rules without distinguishing where the data is held, and to the extent that data is held by a third-party, that too is already addressed (*see Oversight of Third-Party Service Provider Arrangements, above*).

**Model #674, Section 19: The HIPAA Safe Harbor – Recommended Language.** We suggest deleting all of Section 19 and replacing it with the following language to provide more comprehensive protection under the proposed HIPAA Safe Harbor for entities already in compliance with HIPAA’s privacy requirements.

A Licensee in compliance with the privacy rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, HITECH), and which maintains any Nonpublic Information in the same manner as protected health information shall be deemed to comply with the requirements of this Act.

**Model #674, Sections 14, 15, and 16: Adverse Underwriting Decisions.** For health insurers, adverse benefit decisions are already addressed in the NAIC’s *Uniform Health Carrier Review Model Act*, #75 and #76. In the federal Public Health Services Act, Section 2719(b)(1) requires that group health plans and health insurance issuers in the group and individual markets comply with a state external review process if that process includes, at a minimum, the consumer protections set forth in the Uniform Health Carrier External Review Model Act. Also, see 45 CFR 147.136, regarding claims reviews, appeals, and external review processes.

#### **Other Non-HIPAA Concerns.**

AHIP has members which aren’t HIPAA Covered Entities, and many of them have also raised issues unrelated to HIPAA. Since many of them are more granular and less straightforward than the issues we’ve outlined in detail above, we will list some of them in a brief, high-level fashion for now, with the understanding that we will provide you with more information on these topics as we work with you and progress through the Draft Model.

**Model #674, Section 4(A)(5): Data Sharing Limitations.** Our members have concerns pertaining to the restrictions placed on sharing personal information for marketing purposes and research not related to rating or risk management purposes on behalf of the licensee. They also see problems with the restrictions in sharing personal information with a person outside the U.S and its territories.



**Model #674, Section 5(A): Data Retention.** Among other problems, members see a need to include language which makes allowances in the terms of Section 5 depending on the actual feasibility of the requirements due, for example, to the inability of adapting legacy systems to new requirements.

**Model #674, Section 6: Initial and Annual Notices.** This section would require beneficiaries to be notified, raising a number of potential problems, including but not limited to situations in which the identities of beneficiaries of some life insurance policies are intended by the policy owner to be undisclosed.

**Model #674, Section 7: Content of Notices.** This section mandates that notices state a consumer may request a list of any *persons* with which the licensee or third-party service provider has shared the consumer's personal information with the current calendar year, and at a minimum, up to three years prior. This requirement should be made more workable by changing it to *categories of persons*.

**Model #674, Sections 10(B), 11, and 12.** These sections all contain unworkably short time frames for licensees to complete mandated tasks. They all need to be liberalized, as we will detail in future discussions.

**Model #674, Sections 17: Pretext Interviews; and Section 30: Obtaining Information Under False Pretenses.** Our members question whether these provisions are necessary in a privacy model, and would suggest that most state, federal, and common law criminal fraud and insurance fraud laws already address the behavior these provisions are intended to prevent.

**Model #674, Section 21: Confidentiality.** In an area such as this, where the protection of the privacy of sensitive consumer information is the whole purpose, the model should use confidentiality language which most effectively does just that, regardless of whether the information is held by a licensee or the state insurance department. Instead, the Draft Model has included the abbreviated confidentiality language used in the *Insurance Data Security Model Law*, #668. We strongly urge the use of the better choice here, what has come to be recognized as the "Gold Standard" confidentiality language used in the *Risk Management and Own Risk and Solvency Assessment Model Act* (ORSA), #505 (Section 8), and the *Insurance Holding Company System Regulatory Act* (Holding Company Act), #440 (Section 8).

**Section 28: Individual Remedies (Private Right of Action).** The Draft Model has two alternative provisions. Section 28.A neither creates a private right of action nor curtails any private right which might already exist under a state's existing law. Section 28.B specifically creates a private right of action. The policy reasons against this second option and the creation of a new private right of action should be well understood by all interested parties in this effort. Regardless, any model which contains any provision creating a new private cause of action could

not be supported by AHIP, nor its members, at the NAIC or in any state in which the Model was introduced for enactment.

**Recommended Structural Changes.**

Before proceeding to more substantive issues, AHIP recommends the Working Group make or commit to make the following structural changes to the Draft Model.

- Reverse the order of existing model sections 2 and 3.
- Delete existing Draft Model Section 19 and replace it with the recommended Safe Harbor language recommended on page 4.
- Delete Draft Model Sections 14-18 and 30 as their purposes or usefulness in the modern insurance world is unclear, and at least some of them are redundant to other existing law or have little to no relationship to privacy.
- Delete Section 28.B, as it will be broadly opposed by industry and jeopardizes the viability of the Draft Model.

Thank you for the opportunity to provide these comments, and we look forward to further discussing these matters with you in the near future.

Sincerely,

Bob Ridgeway

[Bridgeway@ahip.org](mailto:Bridgeway@ahip.org)

501-333-2621



April 3, 2023

Ms. Lois Alexander  
National Association of Insurance Commissioners  
1100 Walnut Street, Suite 1500  
Kansas City, MO 64106  
Via email to [LAlexander@naic.org](mailto:LAlexander@naic.org)

RE: Comments regarding January 2023 Draft of Consumer Privacy Protection Model Law (#674)

Dear Ms. Alexander:

The American Property and Casualty Insurance Association (APCIA) is pleased to provide the following comments in response to Draft Consumer Privacy Protection Model Law #674 (hereafter "Draft").

APCIA is the primary national trade association for home, auto, and business insurers. APCIA promotes and protects the viability of private competition for the benefit of consumers and insurers, with a legacy dating back 150 years. APCIA members represent all sizes, structures, and regions—protecting families, communities, and businesses in the U.S. and across the globe.

We appreciate the opportunity to share APCIA's thoughts. We recognize that a significant amount of time and work has gone into the initial exposure Draft Model #674, but our members feel significant changes are needed to make this Draft workable.

We understand several of our members have now met with the Privacy Protections Working Group (PPWG) individually and hope that those discussions have given further insight into industry operations that will help this process move forward in an informed and balanced way.

### **Substantive Comments**

Our members have several concerns with this initial draft exposure. We intend to address APCIA's concerns comprehensively, and to provide concrete suggestions, recommendations, and language to address those concerns wherever able. That said, we will have additional feedback on further drafts and as changes are proposed. We look forward to being an active participant in the remainder of this process.

As a starting place, please find below our thoughts on various areas of the draft Model. This letter details several of the major concerns our members have with the current draft, as well as recommendations and language suggestions, where able. As noted, we will have additional technical feedback and proposed language to provide throughout the remainder of the drafting process.

### **Overarching Concerns**

The Working Group's cover letter states that one of the goals in updating this law is to encourage uniformity. However, it is unclear how this proposed Draft would fit with other comprehensive state

privacy laws, and we urge the group to consider an approach that allows for as much harmonization and uniformity between existing requirements as is feasible. A workable draft Model should not contribute to a growing patchwork of conflicting state privacy laws.

In addition, our members are concerned that the Draft requires a disproportionate amount of cost and work compared to the small number of consumers that it will actually benefit. The Draft does not account for older legacy systems that make up a large portion of companies' IT infrastructure and will require companies to implement a large number of manual processes that will be burdensome and costly, and will last for years given the cost and difficulty of migrating to new systems.

### Scope

The Draft appears to apply to any individual who is involved in an insurance transaction, including the insured, claimant, or beneficiary, regardless of whether the insurance service or product is for family, household, or personal purposes. On its face, then, it appears that the Draft could apply to those covered by a policy (for example, employees under a workers compensation policy or drivers on a commercial auto policy). Moreover, the Draft does not appear to account for differences in insurance business models, thereby, for example, treating active writers and run-off specialists the same. If that is the case, many of the requirements of the law become more difficult, and in some instances, such as the provisions related to initial consumer notices practice, unworkable. We would seek clarification on this language.

### Definitions

There are a few undefined terms that are used broadly throughout the letter. These include "sell" and "selling", "actuarial studies", and the terms "marketing" and "research". These concepts are treated very broadly and prescriptively within the draft, and it would be useful to better understand how the Working Groups intends those concepts and what concerns around these topics the Working Group is hoping to address with their inclusion.

We have recommended a few examples of preliminary definition suggestions and edits. In some areas, it is challenging to offer further language suggestions before we receive additional clarification regarding the use of those terms within the draft. However, we hope to be able to provide additional constructive language suggestions in the ongoing discussions during the Working Group calls and in-person meeting.

#### *"Biometric Information"*

- The current definition of "Biometric Information" is overly broad, which would be a serious concern for insurers given the intense uptick in litigation regarding biometrics as a result of the Illinois Biometric Privacy Act (BIPA). It looks like the draft currently takes most of this definition from the definition used in California. We would instead recommend considering the definition included in the Virginia Data Protection Act – "*Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual. "Biometric data" does not include a physical or digital photograph, a video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA.*"

#### *“Control”*

- The definition of “control” inappropriately includes situations where a company may only own 25% of the stock, but does not have the power to control the policies, procedures, or decisions of the “controlled” organization. While in the publicly traded company sphere, 25% may mean more, for private companies where there are often a more limited number of shareholders, there may be a lack of effective control and therefore a lack of ability to direct the “controlled” organization to cooperation with respect to the applicable requirements of the Draft. This should be revised to refer to a majority of the shares owned versus 25%.

#### *“De identified”*

- The law does not seem to address aggregate data. We encourage the definition of de-identified to include aggregated data or, in the alternative, for the law to make clear that personal information does not include aggregate data.

#### *“Insurance Transaction”-*

- We would recommend that the list of appropriate uses for data included in Article II Section 4b be included in the definition for “insurance transaction”.
- We recommend the deletion of the language “any mathematical-based decision that involves a consumer’s personal information.”

#### *“Non-public Information”*

- We recommend deletion of the definition of “nonpublic information”. It is redundant to the definition of “sensitive personal information” in Sec 3 KK and it’s only used one other time in the entire document – in the list of things that make up “personal information in 3 BB (and “sensitive personal information is already in that same list).

#### *“Personal Information”*

- We recommend the Draft exclude “publicly available” information. Not excluding this information would result in significant compliance challenges for the insurance industry. For example, “publicly available” data that is outside the scope of current privacy laws would be subject to Model 674’s right to access, correct, and amend, possibly creating conflicting obligations on insurers, which could result in confusion for consumers in exercising their rights.

#### *“Share, Shared, or Sharing”*

- We request that the definition specifically exclude disclosures to affiliates, disclosures directed by the consumer and disclosures required by compliance with laws and regulations.
- The language “the benefit of any party in which no valuable consideration is exchanged” creates confusion and is challenging to reconcile with the concepts of “renting” or “selling”. We request this language be clarified or, if not necessary, stricken.

#### **Opt-Out vs. Opt-In Approach**

One of our fundamental concerns is the opt-in framework for consent rather than an opt-out framework flips the script on existing data privacy norms by moving insurers and producers from the longstanding opt-out frameworks observed at the state and federal levels to an opt-in model of required consent. Existing laws and regulations, which support an opt-out construct, appropriately balance consumers’ demands for service that is both personalized and expedited with concerns about transparency and the collection, use, and sharing of their personal information. The shift from opt-out to opt-in generates a host of issues,

including the challenge of obtaining consent from individuals who may no longer be customers, for marketing efforts that are a standard business practice and necessary to begin to fill identified coverage gaps, particularly for underserved communities, as well as for online transactions where the user's identity may not be known. Compliance with this Draft would be extremely difficult and damaging to insurers' ability to do business. APCA supports work by the PPWG to modernize and improve the existing data privacy framework for insurance, but believes such work is achievable without disrupting virtually every aspect of the business of insurance.

#### **Requirement of Prior Consent for Overseas Sharing**

Our members feel that this provision in its current form is unworkable. It does not reflect the global, data-driven nature of the insurance business. This provision would either operate as a de facto ban on foreign processing, or it would create two classes of customers, one that can obtain 24x7 servicing and one that cannot.

We note that no existing U.S. privacy law imposes geographic restrictions on processing. The provision here appears to be most closely drawn from the EU's General Data Protection Regulation (GDPR), but consent is not the only legitimate basis for data sharing across borders. GDPR was enacted at a time when many countries did not have mature privacy or data security regulations in place, a much less common occurrence today.

Moreover, this limitation is also contrary to the free flow of data and prohibition on data localization policy positions and commitments adopted by the United States in trade agreements, at the G7, and in its financial regulatory dialogues. The position put forward in the exposure draft to limit the transfer of data outside the United States also is inconsistent with positions taken by global regulatory bodies such as the Financial Stability Board and IOSCO. The free flow of data is not contrary to ensuring data privacy or security. Protecting consumer information is not dependent on the location of where data is stored or processed, or the location of the infrastructure supporting it. Rather, protection is a function of the technologies, systems and internal controls put into place by the companies handling the personal information to protect the data. The position in the exposure draft is not only inconsistent with US policy positions, but is also contrary to the positions adopted by US peer countries such as the EU, UK, Singapore, Japan, and Australia. These governments support the free flow of data, including for personal information, and the need to prohibit data localization requirements while at the same time maintaining privacy frameworks. Singapore, Australia, Japan, the EU and the United Kingdom maintain privacy frameworks without requiring data localization or restricting the free flow of data outside their territories. These countries, like the United States, also have entered into free trade agreements that include commitments to the free flow of data and prohibition on data localization.

It is also imperative that we avoid the imposition of burdensome, impractical rules whose benefits to the consumer are drastically outweighed by the burden imposed on the industry. Our members recommend removing this provision. Our members believe that the type of consent required here would prove both challenging to get and administratively troublesome. For example, if the consumer does not consent or later revokes the consent, licensees and third-party service providers may need to administer these consumer's contracts separately. Further, licensees would need to include this language in the consent at the time of application because it would be difficult to receive consent from consumers after policy issuance.

Imposing new requirements to transfer data outside the U.S., particularly requiring companies to obtain prior consent from individuals to do so, would result in practical and operational challenges. In particular, there would be significant operational impact on companies with global operations, as this new requirement would apply even to intracompany data transfers and data processing activities. It would be

difficult to engage service providers that are located outside the U.S. (or even U.S.-based service providers that have data centers or data processing activities outside the U.S.) to provide services to member companies. Moreover, this requirement would effectively disrupt many existing insurer engagements of non-U.S. vendors, including call centers, that have been in place for years. This would likely have the effect of increasing the cost of insurance by requiring companies to use higher-cost in-country solutions.

Our members would like to better understand the problem the NAIC is hoping to address with this provision. Our members have invested significant resources and effort to transform critical functions using offshore vendors. Such critical functions include customer care and engagement, finance and account management, business analytics and IT security, among others. We believe that if this were implemented, insurers would be less efficient and effective, long term. We are also concerned that this provision also puts insurers in a questionable position when they receive a subpoena or legal equivalent from an entity outside the US and could effectively put insurers in conflict with Section 4 B (4) assuming we will comply with all such legal requirements.

#### **Broadened Requirements for Third-Party Oversight**

Our members believe that the provisions regarding requirements for oversight of third-party service providers are overly broad and prescriptive, as well as unworkable from a contract perspective. We believe this section needs to be significantly reworked, and any additional requirements that do remain should be enacted on a moving-forward basis with a delayed effective date.

In terms of reworking this section, we believe that looking at a more principles-based risk management approach would be a good start. The Draft would require licensees to conduct extensive diligence on third-party service providers and to enter into a written agreement that requires the third-party to comply with both the Draft's requirements for each of the states that adopts the Draft, and the licensee's own practices in connection with the collection and use of consumers' personal information. Applying this extensive and restrictive contractual requirement to all third-party service providers would be unduly burdensome. Additionally, vendors not operating exclusively in the insurance industry may be less inclined to do business with insurers if there are specific industry requirements they need to meet.

We believe it is critical that this Draft not add to the existing contracting burden for insurers, many of whom are still contracting for CCPA and the NAIC's Insurance Data Security Model Law #668. As an alternative, we advocate taking a principles-based risk management approach as was taken in Model #668. We also note that the Draft requires all insurance vendors to comply both with this act (as adopted in each state) and "the licensee's own privacy practices". Our members believe that third-party vendors need the flexibility to set their own privacy practices, which licensees may then choose to accept or decline in accordance with their own risk assessments.

Diversified property and casualty insurance companies disclose personal information to hundreds, if not thousands, of entities that meet the Draft's definition of a third party, each of whom in turn discloses personal information to their vendors and subcontractors. Licensees should not be required to re-negotiate existing contracts to add language specified by the Draft. Instead, the Draft should establish standards for third party contracts that ensure personal information is protected without requiring them to include specific language. For example, standard vendor contracts typically contain language requiring the vendor to preserve the confidentiality of personal information and prohibiting the vendor from using personal information for the vendor's own purposes. This should be sufficient to ensure that personal information is not misused by a licensee's vendors.

### **Additional Permitted Transactions and Actuarial Studies**

We note that the Draft requires prior express consent for the use of personal information for "additional permitted transactions". Our members find this problematic, particularly given the broad application of these undefined terms, but also for the reasons set forth above—other privacy regimes generally use opt-out rather than consent-based frameworks. As we have noted elsewhere, actuarial studies are lumped in with "additional permitted transactions" in places throughout the draft. For instance, the Draft's provision regarding allowable uses for "additional permitted transactions" appears to redefine the term by adding "actuarial studies," even though actuarial studies were not part of the definition for "additional permitted transactions." We believe the definition which distinguishes between these types of activities is correct. Actuarial studies are not research activities, especially when they are performed by the licensee itself. Rather, actuarial analysis is a core part of insurance processing. Our members note this distinction is critical, and that actuarial studies and analysis should be treated as a core part of insurance processing and not subject to onerous and prescriptive restrictions.

There appears to be some internal inconsistency throughout the draft regarding actuarial studies. In the "Definitions" section, activities related to risk management, such as actuarial studies, are included in the definition of an insurance transaction. Additionally, the definition of "additional permitted transactions" explicitly excludes research activities related to rating or risk management purposes, which would as a result exclude actuarial studies. However, in other places throughout the document actuarial studies are lumped with marketing and research and made subject to the same requirements of prior consent [see Article II, Section 4 (E)(1)]. It is critical that actuarial studies be distinguished from these other issues, as they are inherently very different from general marketing and research activities. Actuarial studies are essential for insurers and critical to risk management.

We also note that Article III, Section 7(A)(7)(b) and (c) require consent for personal information to be used for actuarial purposes unless deidentified and for research. As with the consent for personal information shared with persons outside the US, licensees would need to include this language in the consent at the time of application because it would be difficult to receive consent from consumers after policy issuance. This could impair the ability to perform important pricing research or skew actuarial studies. We would raise for your attention the inconsistency with how actuarial studies are addressed throughout the document and note that they should not be subject to any prior consent requirement.

### **Marketing**

As previously noted, the Draft requires prior express consent for use of personal information for "additional permitted transactions", including marketing and research activities. The Draft's restriction on marketing is unprecedented and should be tailored to regulate practices that the Working Group is particularly concerned about. The Draft would prohibit a licensee from processing personal information for "marketing" unless the consumer first provides prior express consent. This would make some forms of traditional, first-party marketing impossible. For example, a licensee would not be able to target solicitations to any individual with whom the company has no prior relationship and where it is impossible to obtain prior consent.

The rule is also too vague, as the term "marketing" could be read to encompass routine interactions with consumers during the application, claim, and quote process, such as cross-selling, recommendations regarding coverage, etc. We also note the potential ambiguity and the broad usage of the concept of marketing throughout the Draft, and seek further clarification on the root concerns the Working Group hopes to address with these provisions. Insurers should be permitted to market without prior consent and



with a consumer option to opt-out, consistent with existing federal standards. We also have considerable concerns with the potential implications for joint marketing, and have further addressed those below.

### **Joint Marketing**

Joint marketing with other financial institutions is an essential part of many insurers' business models and a critical means of providing consumers access to products, which would be prohibited under the Draft. The Gramm-Leach-Bliley Act (GLBA) offers an explicit framework for financial institutions to engage in joint marketing, enabling one trusted financial institution to share the nonpublic personal information of customers with another financial institution for the limited purpose of jointly offering financial products or services. Under GLBA and its implementing regulations, participating financial institutions must undertake certain privacy protections and security safeguards to share and use nonpublic personal information in joint marketing programs. Further, the financial institutions must enter a contract which limits the use of shared nonpublic personal information to the joint marketing program. GLBA requires financial institutions to provide notice to individuals that their information will be shared for joint marketing.

Joint marketing leverages consumers' trust in their financial institution to raise awareness and increase access to important financial products and services, particularly for the underserved. As the NAIC undertakes various workstreams aiming to identify and fill coverage gaps and ensure the availability of financial products and services for all consumers, joint marketing plays an important role.

The Draft prohibits joint marketing through requirements for prior consent for marketing such as in Section 4(A)(5)(a), 4(E), and 4(G), among other sections. Insurers participating in joint marketing programs do not own a primary relationship with the customer, so there is no opportunity to provide prior notice or choice directly as would be required by the Draft. Further problematic, the Draft requires only insurance companies to obtain prior consent. As a result, the Draft decouples insurance regulation from longstanding GLBA rules and disadvantages insurance products as compared to other financial products and services.

It is appropriate and necessary that insurers be allowed to continue this critical business practice which is already limited to financial institutions. APCA requests that joint marketing be clearly exempted from any new or additional marketing requirements contemplated in future versions of the Draft.

### **Private Cause of Action**

We strongly oppose the inclusion of an optional private cause of action. We believe enforcement is most appropriately handled by state insurance regulators and that state insurance departments should be designated as the exclusive enforcement mechanism.

The complexity and sheer breadth of the Draft in its current form ensure that violations are inevitable. Other privacy-related statutes that allow private causes of action with statutory damages, such as the California Invasion of Privacy Act and the Illinois Biometric Privacy Act, have spawned an entire industry of plaintiff's class action litigation even though the conduct regulated by those laws is relatively narrow. By contrast, the Draft touches almost every facet of a licensee's operations, making it virtually impossible for companies to shield themselves from liability. Our members believe that insurance departments are well-equipped to set expectations and resolve thorny interpretative issues through enforcement.

We also note that the privacy space is already heavily regulated at both the state and federal level, and insurers are subject to numerous market conduct, financial, and other exams that cover privacy. In addition, the increasing cost of litigation is already a major cost driver for insurance, and continuing to

unnecessarily drive up that cost will make insurance coverage less accessible to consumers. Our members believe the more efficient approach to addressing violations is an administrative process enforced by state departments of insurance. Those processes are better for consumers and regulated entities in comparison to litigation. A private cause of action would increase costs for society at large, and the benefit to consumers would be small in comparison. This is another area of the draft where we feel the appropriate balance has not been struck. Therefore, we strongly recommend the “optional” private cause of action be removed.

### **Notice Requirements**

APCIA believes that privacy notices should be readable and accessible so that consumers truly read and understand their rights. Our members believe that the additional notice requirements imposed in the draft will do just the opposite. The Draft would expand privacy notice and disclosure requirements to consumers, which are already complex and lengthy. The draft does not include a safe harbor when using the Federal Model Privacy Form (defined under the Gramm-Leach-Bliley Act) which many insurers currently use. The Draft should contain such a safe harbor.

In addition, to eliminate privacy notice confusion and streamline consumer notice requirements, the Draft should align with the NAIC’s 2016 Gramm Leach Bliley Act Annual Privacy Notices Bulletin. Following Federal passage of the FAST Act and adoption of the NAIC bulletin, 42 states either adopted the bulletin or required law and rule changes to eliminate GLBA annual notices provided certain conditions are met to “eliminate a duplicative and costly notification requirement”. We recommend the Draft similarly only require subsequent annual notices if there is a material change.

Our members can appreciate the need for a publication of the notice on the licensee’s website and perhaps even some sort of consumer communication if the notice is materially modified. The most effective method of delivery and ensuring that the consumer has ready access to the current notice is for it to be posted on the licensee’s website. Posting to a website could also alleviate concerns with respect to delivering an initial notice to consumers, particularly where the carrier does not have a direct relationship with the consumer. The current options for electronic delivery described in the Draft are challenging because of the requirement to obtain an acknowledgement from each consumer if they view the notice electronically or to get an email delivery receipt. In terms of the latter, consumers can block delivery receipts, which complicates this process.

### **Data Minimization**

APCIA members are concerned that applying the included data minimization standards to situations where an insurer already has information and retains it after implementation could be quite problematic. Specifically, our members believe that information kept in legacy systems or formats, or otherwise part of in-force business, should be kept out of scope. Requiring affirmative consumer opt-in consent before continuing with current activities could result in unintended consequences for consumers, including service disruptions. We note that this, like several other provisions of this act, would have significant systems implications and in many cases effective and appropriate change management will be challenging. In general, APCIA believes that the Draft’s rules for processing personal information are unnecessarily restrictive. We are also concerned about how reinsurance would fit in here, and would seek clarification of whether reinsurance would be considered “servicing”. We recommend the inclusion of language clarifying that sharing of information is permitted for reinsurance purposes.

Further concerning, Draft provisions in Section 4(A) that prohibit licensees from engaging in the collection,

processing, retention, or sharing of a consumer's personal information unless in connection with an insurance transaction may have unintended consequences for licensees' non-insurance products and services. The provision could be read to prohibit licensees from offering non-insurance products, at least to the extent such offers require the processing of personal information. For members that offer consumers a mix of both insurance and non-insurance products and services (e.g., vehicle service contracts and GAP waiver) for holistic financial planning, the prohibition could have significant negative impacts on available offerings.

### **Retention and Deletion**

Our members appreciate the inclusion of language that addresses the need to retain information in compliance with their legal obligations. However, we recommend deleting the references to "applicable to any insurance transaction" within that section. Insurers need to retain data in compliance with all applicable legal obligations, not just those legal obligations applicable to insurance.

The application of deletion requirements to legacy systems that were never designed to automate deletion is extremely challenging and, in some cases, technically infeasible due to technological limitations. In many cases, these systems contain records that either cannot be deleted manually due to volume, or where automated deletion may not be an option due to legal or litigation holds. Regarding the latter, it should be noted that class action litigation is often broadly defined in many different ways to apply to not just individual insurance policies (with unique numbers), but also to broad classes of policies that may be impossible to reconcile with automated deletion solutions.

It would be difficult to overstate the cost of implementing a data retention program with the granularity the initial Draft appears to require. Insurers are subject to a variety of state laws that establish different minimum retention periods and also need to implement exceptions to retention periods to preserve data that may be subject to litigation or other regulatory requirements. Read literally, the Draft would require a company to delete each individual record (or de-identify it) within 90 days of when the applicable state-prescribed retention period expires. This is well beyond the capacity of most, if not all, existing underwriting and claim systems, to say nothing of unstructured data in email, online documents, file shares, etc. Further, the obligation to notify consumers when personal information is deleted does not contemplate long-tail policies, where personal information may be retained for 10+ years. If this requirement is retained, insurers must develop costly tracking processes to maintain their consumers' address, who frequently relocate, change their name, etc. The Draft should instead impose a standard that balances the consumer's interest in data minimization with the significant cost of purging data on a defined schedule and the feasibility of notifying consumers of the deletion.

The specificity of this rule is a significant deviation from the principles-based approach in insurance data security regulations and state privacy laws. The NY DFS Cyber Regulation, for example, allows insurance companies to weigh business need, security, and risk in crafting retention policies. CCPA requires companies to articulate the "criteria" used to establish retention periods. We recommend harmonization with these principles-based approaches. As opposed to a prescribed 90-day period of time, we would suggest that licensees have retention policies available for examination and that companies be required to retain and delete information subject to their retention schedule. We do not believe a one-size-fits-all approach is appropriate. We would again seek clarification of the expectation regarding requirements for vendors to delete personal information. If a licensee informs a vendor that it is required to delete data, is that sufficient to be in compliance with these requirements?

### **Access and Correction**

We note that the current response time for requests for access and correction in the Draft are 15 days, which is unworkable and go far beyond any other existing legal standard. Even the most technologically advanced companies would be challenged to meet those requirements, and many insurance carriers work with legacy information systems that make this impossible to comply with. These are very abbreviated response times, particularly for requests requiring a substantive response, and should be extended.

By way of comparison, the existing state consumer privacy laws generally afford licensees 45 days from the date of receipt to respond, with the option to extend the response period for an additional 45 days when reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the controller informs the consumer of any such extension within the initial 45-day response period, together with the reason for the extension. Each state consumer privacy law allows a licensee to charge to a fee for multiple requests to exercise the same right within a 12-month period or to deny such request for being excessive. Such options should be included in this law as well.

Finally, the Draft should delete the requirement to include a consumer's statement if a correction request is denied. Modern, electronic exchanges of data are rigidly formatted and don't lend themselves to transmission of a free-form statement. Moreover, it's unlikely to be read by human eyes.

### **Adverse Underwriting Decisions**

The Draft includes provisions related to "Adverse Underwriting Decisions". Our members do not believe this Draft is the appropriate place to address those issues. We note that the NAIC Transparency and Readability (C) Working Group is working on a separate work product to address this. We would appreciate clarification on how this section is different from the work being done in that group and why it is necessary as an addition, to understand better how this is not duplicative of those efforts. Our members recommend removing this section and allowing the NAIC Transparency and Readability (C) Working Group to continue addressing these issues in that forum.

### **Process Feedback**

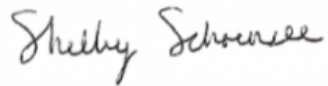
We joined many of our industry partners in the request for an in-person stakeholder drafting session. We appreciate the NAIC agreeing to hold this session, which we believe will be invaluable to efficiently and effectively working through some of the thornier issues in this draft. We also appreciate the scheduling of regular open calls throughout the remainder of the drafting process. APCIA will be actively engaged in providing constructive feedback during these opportunities. We hope that these next steps will encourage future versions to better reflect a balance between the need for consumer protection and the need for insurers to be able to provide their products and services in a workable way. It is only through continued communication between the regulator and regulated communities that a balance between the need for appropriate oversight and operational flexibility can be achieved. We are also happy to further discuss our concerns and suggestions with the Working Group and its members, and look forward to actively engaging in the upcoming calls and meetings where industry can provide concrete, constructive feedback.

### **Conclusion**

APCIA thanks the Working Group for its consideration of our comments. In this letter, we aimed to address several of our major concerns with the draft more comprehensively and provide constructive suggestions wherever able. That said, we will have continued feedback on various pieces of the draft as we continue through the drafting process. We very much appreciate the scheduling of additional open calls and an in-

person meeting, and plan to be fully engaged in the open stakeholder process as this Draft continues to develop. We are happy to discuss any of the concerns or suggestions included therein further, and look forward to working with you all thoughtfully to achieve a balanced final product that will be workable for all stakeholders.

Sincerely,

A handwritten signature in cursive script that reads "Shelby Schoensee".

Shelby Schoensee  
Director, Cyber & Counsel



1310 G Street, N.W.  
Washington, D.C. 20005  
202.626.4800  
www.BCBS.com

April 3, 2023

Katie C. Johnson, Chair  
Cynthia Amann, Co-Vice Chair  
Chris Aufenthie, Co-Vice Chair  
NAIC Privacy Protections (H) Working Group  
Attn: Lois Alexander, Market Regulation Manager II  
Via email: [lalexander@naic.org](mailto:lalexander@naic.org)

**RE: Exposure Draft of the Consumer Privacy Protections Model Law (#674)**

Dear Chair Johnson, Co-Vice Chairs Amann and Aufenthie, and Members of the Working Group:

The Blue Cross Blue Shield Association (BCBSA) appreciates the opportunity to respond to the Privacy Protections (H) Working Group's (Working Group) Exposure Draft of the new Consumer Privacy Protections Model Law #674 (Draft Model).

BCBSA is a national federation of 34 independent, community-based and locally operated Blue Cross and Blue Shield (BCBS) companies (Plans) that collectively provide healthcare coverage for one in three Americans. For more than 90 years, BCBS Plans have offered quality healthcare coverage in all markets across America – serving those who purchase coverage on their own as well as those who obtain coverage through an employer, Medicare and Medicaid.

We applaud and appreciate the Working Group's efforts to initiate a collaborative process where states and interested parties can participate in future drafting sessions in the next phase of the model development. We have participated in many discussions with the Working Group on consumer privacy protections and know that this issue is very important to regulators, as it is to all the members BCBS companies serve. It is with this in mind that we offer recommendations that reflect the work BCBS companies do to ensure consumer privacy protections and secure use of consumer data.

We appreciate that the Draft Model is consistent with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) standards in several areas; however, as currently drafted,

the model does not extend these HIPAA protections to all aspects of the regulatory scope. As explained in more detail below, we wish to highlight the following key recommendations:

**Maintain a HIPAA and HITECH Safe Harbor:** We support the Draft Model’s exemption of health insurers through a “safe harbor” provision set forth in Section 19, “Compliance with HIPAA and the HITECH.” As the drafters likely considered in developing Section 19, health insurers and healthcare companies that are covered entities under HIPAA are already subject to extensive and evolving data privacy protection requirements under HIPAA, the Health Information Technology for Economic and Clinical Health (HITECH) and other federal laws. Given the unnecessary duplication of efforts and administrative complexities that additional requirements beyond HIPAA and applicable federal laws would present to health insurers and individuals, we respectfully request that HIPAA compliant entities be deemed in compliance with this provision in the final version of the model.

**Align with HIPAA Standards Where HIPAA Does Not Apply.** To the extent that health insurers already subject to HIPAA are not exempt from a provision in this Draft Model, such provision should align with HIPAA. We believe alignment will ensure that consumers remain protected while balancing health insurers’ business needs to function under a consistent regulatory environment. For instance, we respectfully call attention to the [Virginia Consumer Data Protection Act of 2021](#) (Va. Code Ann. § 59.1-576(B) 2021), which exempts covered entities or business associates governed by HIPAA, HITECH or subject to the Gramm-Leach-Bliley Act, and where the state has recognized the extent to which the HIPAA regulatory and enforcement regime requires health insurers to safeguard protected health information.

Further, reliance on existing requirements is essential to ensure that health insurers can consistently apply one set of standards and reduce operational and compliance challenges that are confusing to both consumers and health insurers, add administrative burden and costs without adding meaningful protections for consumers, and may inadvertently result in damage to consumer data privacy. Given these unintended consequences, a safe harbor will avoid potential ambiguities and inconsistencies, while reinforcing the existing health privacy regulatory regime and enabling stronger compliance with consistent consumer data privacy protections across the healthcare industry.

To ensure that the safe harbor in Section 19 is applied consistently throughout the Model Law, we recommend the following changes that extend the safe harbor to Sections 9 through 12:

- **Add the following language (underlined and in red font) to Article III, Notices and Authorizations, Section 9(A), Consumers’ Consent – How Obtained:**
  - A. Where the consumer’s consent for the collection, processing, or sharing of consumers’ personal information by a licensee is required by this Act, a licensee shall provide a reasonable means to obtain written consent and maintain a written record of such consent. For licensees subject to HIPAA and HITECH, pursuant to

Section 19, consent requirements shall be consistent with those provided under HIPAA and HITECH.

HIPAA permits, but does not require, a covered entity to obtain consent from a consumer for uses and disclosures of PHI for treatment, payment, and healthcare operations. However, consumer authorization is required in certain circumstances, such as for purposes beyond treatment, payment, and healthcare operations. A valid authorization must provide the individual with a right to revoke their authorization at any time, provided that the revocation is in writing, except in two very narrow circumstances: (1) the health insurer has taken action in reliance thereon; or (2) if the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.<sup>1</sup>

In addition, a Notice of Privacy Practices is required under HIPAA. This notice, which must be made available to health plan members at the time of enrollment as well as annually, describes, among other things, the right an individual must restrict the use and disclosure of their PHI for even core treatment, payment and operations purposes, as provided by the HIPAA Privacy Rule.

- **Add the following language (underlined and in red font) to Article IV, Consumers' Rights, Section 11(A), Access to Personal Information:**
  - A. Any consumer, after proper identification, may submit a written request to a licensee for access to their personal information in the possession of the license. Access requests submitted to a licensee or third-party service provider subject to HIPAA or HITECH shall be governed by applicable federal and/or state law.

HIPAA grants consumers the right to access their PHI in designated record sets upon request from their providers and plans (i.e., covered entities) as well as those maintained by business associates.<sup>2</sup> Designated record sets include, without limitation, information such as medical records, billing records, claims records and health enrollment records. Covered entities are only required to provide consumers access to the PHI that the consumer specifically requests. The HIPAA right of access regime is very well-established and should continue to govern requests for access to PHI from consumers to their health plans. Imposing different standards will create even more confusion for health insurance entities that are already subject to varying state law requirements regarding consumer access rights.

- **Add the following language (underlined and in red font) to Article IV, Consumers' Rights, Section 12(A), Correction or Amendment of Personal Information:**

---

<sup>1</sup> 45 C.F.R. §164.508(b)(5).

<sup>2</sup> 45 CFR §164.524.



- A. Any consumer, after proper identification, may submit a written request to a licensee to correct or amend any personal information about the consumer within the possession of the licensee. Amendment requests submitted to a licensee or third-party service provider subject to HIPAA or HITECH shall be governed by applicable federal and/or state law.

Under HIPAA, an individual has the right to correct (i.e., amend) PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set.<sup>3</sup> As a covered entity, the health insurer must act on the individual's request for an amendment no later than 60 days after receipt of such a request. Any denial to correct by the health insurer must have a basis authorized by the regulation and be communicated to the individual. If the individual disagrees with the denial, the individual may file a statement and/or a complaint to the health insurer or the U.S. Department of Health and Human Services. Otherwise, the information must be corrected in the manner provided in the regulation, such as through informing recipients of the corrected information including business associates.

In addition, we recommend the following changes to the existing HIPAA/HITECH safe harbor in Section 19 of the Draft Model:

- **Incorporate the following language (underlined and in red font) and edits (strikethroughs) in Section 19, Compliance with HIPAA and HITECH:**

- A. A licensee or third-party service provider that is subject to and compliant with the Privacy, Security, and Breach Notification Rules issued by the United States Department of Health and Human Services (HHS), Parts 160 and 164 of Title 45 of the Code of Federal Regulations, ~~established~~ pursuant to the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Public Law 111-5, HITECH), and collects, ~~processes uses~~, retains, ~~and shares or shares~~ all personal health information in the same manner as protected health information:

(1) Shall be deemed to comply with Sections 4-~~12~~8 of this Act provided:

(a) The licensee obtains the consent of the consumer prior to engaging in any additional permitted transactions; as defined in this Act, where the additional transactions are outside the scope of HIPAA treatment, payment, and healthcare operations. ~~and~~

~~(b) The licensee obtains all necessary consent of consumers' whose personal information is shared with a person outside the jurisdiction of the United States or its territories, as provided in this Act; and~~

---

<sup>3</sup> 45 C.F.R. §164.526.

- (2) Must comply with the remaining sections of this Act, where as applicable.
- B. The licensees shall submit to the [Commissioner] a written statement certifying that the licensees comply with the requirements of Subsections A of this section.
- C. Subsections A and B of this section shall continue to apply to such licensee if the [Commissioner] in consultation with affected licensees has not issued a determination finding that the applicable federal regulations are materially less stringent than the requirements of this Act and if the licensee has complied or made reasonable efforts to comply with the requirements of this section.

These changes reflect the reality that alignment of existing consumer data requirements with HIPAA and HITECH continues to grow in importance in the healthcare ecosystem.<sup>4</sup> Such alignment will ensure that the same robust privacy protections apply to the same type and use of health information, no matter the jurisdiction, and mitigate duplication and conflict between federal and state requirements.

In the above recommendation, we added “third-party service provider” because third-party service providers (e.g., business associates under HIPAA) must agree to use the consumer information according to certain conditions and under circumstances in a business associate agreement. These business associates are also subject to HIPAA confidentiality and privacy protections. Given their equal exposure to consumer data as licensees, as well as HIPAA’s direct applicability to business associates including the potential for federal enforcement actions against the business associate directly, third-party service providers should be afforded the same carve-out as licensees to further align the Draft Model with HIPAA.

Second, in Section 19(A)(1), consistent with our comments to Sections 9-12 above, we expanded the applicability of the carve out to Sections 9-12 of the Draft Model because HIPAA already regulates these domains. We added language in Section 19(A)(1)(a) to clarify that, consistent with HIPAA, consumer authorization is required for purposes beyond treatment, payment, and healthcare operations.

Finally, we revised Section 19(C) because allowing for a post hoc determination by the Commissioner without consultation with affected health insurance entities would create instability and disruption to health insurers’ operations with little notice or stakeholder feedback. In the unlikely event that a federal law applicable to HIPAA covered entities and business associates is enacted, representatives from health insurance entities in consultation with the Commissioner would be in the best position to re-assess the applicability of Sections 19(A) and (B). We respectfully ask the Working Group to reconsider this provision.

---

<sup>4</sup> For example, the U.S. Department of Health and Human Services Office for Civil Rights and the Substance Abuse and Mental Health Services Administration recently issued a proposed rule that would align 42 CFR Part 2, which outlines confidentiality protections for substance use disorder records, with HIPAA privacy rules. 87 FR 74216.

We would like to thank the Working Group for its consideration of our comments and look forward to continuing to work with you on refining this Draft Model. If you have any questions, please do not hesitate to contact BCBSA's managing director, state affairs, Randi Chapman at [randi.chapman@bcbsa.com](mailto:randi.chapman@bcbsa.com) or managing director for health data and technology policy Lauren Choi at [lauren.choi@bcbsa.com](mailto:lauren.choi@bcbsa.com).

Sincerely,

A handwritten signature in black ink that reads "Clay S. McClure". The signature is written in a cursive, flowing style.

Clay S. McClure  
Executive Director, State Affairs

April 3, 2023

Chair Katie Johnson (VA)  
Vice Chairs Cynthia Amann (MO) and Chris Aufenthie (ND)  
2023 NAIC Privacy Protections (H) Working Group  
NAIC Central Office  
1100 Walnut Street  
Suite 1500  
Kansas City, Missouri 64106

Sent via email to: [lalexander@naic.org](mailto:lalexander@naic.org)

**RE: Insurance Consumer Privacy Protection Draft Model Law #674 (Model #674)**

Dear Chair Johnson and Vice Chairs Amann and Aufenthie:

The Committee of Annuity Insurers (CAI)<sup>1</sup> appreciates the opportunity to submit the following comments to the 2023 NAIC Privacy Protections (H) Working Group (Working Group) on the exposure draft of Model #674. In providing our comments at this stage, we applaud the Working Group's efforts to date on this complex and important issue, and its commitment to continuing to work collaboratively over the coming months with consumer and industry stakeholders in order to craft effective and pragmatic enhancements to consumer privacy protections that are tailored to the insurance sector.

**OVERVIEW**

While the CAI recognizes and supports the importance of making tailored updates to the privacy rules governing the insurance sector, we are concerned that the current draft of Model #674 would meaningfully limit the ability of the insurance sector to compete within the broader financial services markets. The insurance industry, along with the banking and securities industries, comprise the three main branches of the financial services sector in the United States. These three branches are highly interconnected in providing services to consumers and all three branches have been subject to largely consistent rules under the Gramm-Leach-Bliley Act (GLBA) regarding the privacy rights that they offer to those consumers.

As proposed, Model #674 would dramatically change this equilibrium by placing much stricter limitations on licensees' ability to process their consumers' data relative to the banking and securities sectors. This would put CAI members and all insurers at a competitive disadvantage in the broader marketplace for financial products, including by prohibiting their use of certain personal information even with the consumer's consent; increasing costs for insurers by reducing their access to offshore service providers; and reducing the ability of insurers to market new products, even to existing consumers.

As you continue to work on the draft Model #674, we urge you to be mindful of the balance between protecting consumers and enabling the smooth and efficient operation of insurance businesses that provide necessary and important financial protection and tools to those consumers. Consumers understand that licensees need to collect personal information to provide them with the

---

<sup>1</sup> The Committee of Annuity Insurers is a coalition of life insurance companies that issue annuities. It was formed in 1981 to address legislative and regulatory issues relevant to the annuity industry and to participate in the development of public policy with respect to securities, state regulatory and tax issues affecting annuities. The CAI's current 31 member companies represent approximately 80% of the annuity business in the United States. More information is available at <https://www.annuity-insurers.org/>.

financial products and services they request and to operate their businesses. We suggest that Model #674 should be tailored to the needs of the insurance sector specifically and to reflect consumer expectations in our industry. Our comments below focus on several significant aspects of the draft Model that CAI members believe warrant particular attention in this regard.

## COMMENTS

### **1. The data minimization limitations, including consent requirements for marketing, would limit the ability of licensees to compete in the marketplace and innovate in the future.**

Section 4 of the Model Law on "Data Minimization and Sharing Limitations" would limit the ability of insurance licensees to collect, process, retain, or share personal information collected in connection with providing an insurance product or service to a few narrow circumstances. This would include only being able to use data for marketing or internal research purposes (defined as "additional permitted transactions")<sup>2</sup> with prior express consent. Section 4 would prohibit any use of the information that does not fall under the definitions of an "insurance transaction" or "additional permitted transactions." This approach sets narrow limits on the purposes for which data may be used, without providing consumers the ability to consent to additional uses. Taking this approach would disrupt current business practices and create additional costs that would necessarily be passed on to consumers. It would also limit the ability of the insurance industry as a whole to innovate, since the use of personal information would be limited to only the seven enumerated uses.

We are also concerned about the breadth of Section 4(G) as proposed, in that it broadly prohibits any licensee from collecting, processing, retaining, or sharing any personal information "in a manner inconsistent with the direction of a consumer . . . ." While it is unclear what the intent of this provision is, as drafted it would subject licensees and their ability to conduct business to the whims of each consumer. For example, a consumer could direct a licensee to only process their personal information for claims or marketing on Tuesdays and the licensee would be bound by that direction. This provision would also allow consumers to constrain the ability of licensees to retain their data, thereby creating a shadow deletion right within the Model. This provision should be deleted.

The requirement to obtain affirmative consent prior to using personal data for marketing to a licensee's own existing customers, would be particularly disruptive to current business operations. It would also functionally prohibit joint marketing with trusted financial institutions and limit the ability of licensees to inform consumers of the beneficial products and services they may need. Consumers may not take the time to provide marketing consent, not because they are necessarily opposed to receiving marketing but because they would not take the extra step necessary to provide consent. This would upend the basic business model of how many licensees market their products, hampering their ability to grow and maintain their businesses.

Because the restrictions of the draft Model are stricter than any other current or pending US privacy law (such as the California Consumer Privacy Act), including those that govern other financial services sectors, it would place the insurance industry as a whole at a competitive disadvantage with competing non-insurance financial products. For example, SEC-regulated broker-dealers and investment advisors that sell both annuities and competing non-insurance products (such as mutual funds or CDs) would be able to market the non-insurance product to a consumer readily, but would require consent to market an annuity product that may be a better fit to the same consumer. This imbalance would mean that broker-dealers and advisers would be more likely to offer non-insurance products to consumers, and create an asymmetry of information in the marketplace that would function to drive consumers away from insurance products that may better meet their needs. The CAI

---

<sup>2</sup> "Additional permitted transactions" means "collecting, processing, retaining or sharing a consumer's personal information, with the consumer's consent, for: (1) marketing purposes; or (2) research activities not related to rating or risk management purposes for or on behalf of the licensee." Section 3.B.

supports providing tailored privacy enhancements to insurance consumers, but suggests that it can be done without affecting the competitiveness of the insurance industry.

The rational underlying modern privacy regulation is based on two basic tenets: (1) consumers should be able to understand where their personal information goes and how it will be used; and (2) consumers should be able to exercise control over their personal information. We suggest that a revised version of the Model could achieve these goals without affecting the ability of licensees to compete in the market or innovate for the future.

*CAI Recommendations.* Instead of narrowly defining the permitted purposes for which personal information may be used, the Model should be revised to empower consumers to choose how their personal information may be used by exercising opt-out rights, and to allow purely internal uses of personal data.

To that end, the data minimization restriction should be limited to requiring that any collection, use, and processing of personal information must be reasonably necessary and proportionate to achieve the disclosed purposes for which it was collected. Separately, consumers should be able to opt-out from having their personal information used to market to them, or shared with non-affiliated third parties other than as necessary to administer a requested service (consistent with current Model #672). Purely internal uses of personal information that are properly disclosed should be permissible. We believe this approach would appropriately balance the interest of licensees in operating their businesses and offering beneficial insurance products into a competitive market with the rights of consumers to exercise control over their personal information.

## **2. The prohibition on using and sharing sensitive personal information for marketing and research, even if the consumer consents, is overly restrictive.**

Section 4.E.(2)(b) of draft Model #674 would prohibit the sharing<sup>3</sup> of “sensitive personal information”<sup>4</sup> for marketing or any other “additional permitted transaction,” even if the consumer consents to such sharing and use. It is common practice to use sensitive personal information to enhance digital marketing. Because the definition of sensitive personal information is so broad (it is similar to the definition found in the California Privacy Rights Act), the prohibition on the use of sensitive personal information in marketing would put insurers at a competitive disadvantage relative to other financial institutions’ marketing activities that are not similarly constrained. This section would also limit the kinds of research an insurer can undertake to understand its business, including internal research into the impacts that certain insurance practices are having on various protected classes.

No other privacy law in the United States flatly prohibits the use of sensitive personal information in advertising or research. For example, the California Consumer Privacy Act requires that consumers be given notice and the opportunity to opt-out of the use of their sensitive personal

---

<sup>3</sup> “Sharing” is defined broadly to include “disclosing, disseminating, making available, releasing, renting, transferring, selling or otherwise communicating by any means a consumer’s personal information...” Section 3.LL.

<sup>4</sup> “Sensitive personal information” is defined broadly to mean “information that reveals (i) a consumer’s social security, driver’s license, state identification card, or passport number; (ii) a consumer’s account log-in or financial account, debit card or credit card numbers in combination with any required security or access code, password, or credentials allowing access to an account; (iii) a consumer’s precise geolocations; (iv) a consumer’s racial or ethnic origin, religious or philosophical beliefs; (v) union membership; (vi) the contents of a consumer’s personal mail, personal email, and personal text messages unless the person in possession is the intended recipient of the communication; (vii) a consumer’s genetic data; (viii) a consumer’s sex life or sexual orientation; (ix) a consumer’s citizenship or immigration status; (x) a consumer’s health information; or (xi) a consumer’s biometric information.” Section 3.KK.

information for marketing. Similarly, no other U.S. privacy laws prohibit the use of sensitive personal information for research purposes.

Section 4.E.(2)(b) of Model #674 would also prohibit the sharing of sensitive personal information with affiliates for marketing purposes, even if no consideration passes between the parties. However, Section 4.I. of Model #674 contains one exception to the affiliate sharing prohibition. That section acknowledges the federal preemption language found in Section 625 (b)(1)(H) and (b)(2) of the Fair Credit Reporting Act ("FCRA") that prohibits the laws of any state from imposing any requirement or prohibition on select provisions of the FCRA. Those sections in turn reference FCRA's Section 624 Affiliate Sharing that, in effect, requires companies to (a) provide prominent disclosure to consumers that information about them in a consumer report may be communicated to an affiliate for marketing purposes and (b) give consumers a simple method for opting out of such marketing.

*CAI Recommendation.* Section 4.E.(2)(b) of Model #674 should be revised and brought in line with other privacy laws enacted at the federal or state level.

**3. The prohibition on processing personal information outside the United States without obtaining consumer consent would adversely limit the ability of licensees to choose the best service providers and would increase costs for consumers.**

Section 4.C. of the draft Model would prohibit licensees from sharing personal information with, or collecting or processing personal information through, an entity outside of the United States. Because it is unlikely that licensees would be able to obtain consent from all or even most consumers as a practical matter, this provision would function as a general prohibition on processing personal information outside of the US, including through domestic vendors. As a result, this requirement would disrupt existing business operations and relationships, triggering costs to create on-shore alternatives to existing offshore vendors. These costs would necessarily be passed on to consumers. It would also limit the ability of licensees to use cloud-based vendors and otherwise choose the best available service providers in the market, since many service providers simply do not allow for customers to limit data processing only to the US.

There are alternative means to protect consumers without limiting the ability of personal data to be processed outside of the U.S. The use of offshore vendors to process personal information is a common business practice that provides a range of consumer benefits, including enabling extended hours of customer support, reduced costs, and increased system resilience. Requiring consumer consent also would not directly address the risks posed by offshore data processing. Privacy laws like the EU GDPR that do establish limitations on transferring data to an outside jurisdiction do so to avoid offshore processing being used to avoid complying with onshore privacy requirements. To that end, the GDPR does not require consent to allow offshore processing or otherwise prohibit offshore processing, but rather establishes requirements that ensure that data will be adequately protected even when processed offshore. Likewise, Model #674 can protect consumers when data is processed outside of the United States by requiring licensees to exercise oversight of offshore vendors and to enact appropriate contractual protections based on the risk of the vendor. Indeed, doing so is already a common practice within the insurance market.

*CAI Recommendation.* The requirement to obtain consumer consent prior to processing data outside the US should be deleted. Rather, the Model should rely on appropriate third-party service provider oversight obligations to require that licensees perform appropriate due diligence on all service providers, including offshore service providers. This should include a requirement to ensure that any data processed by an offshore service provider is, via contract or otherwise, subject to the oversight provisions in the Model (see discussion below in Section 5). Taking this approach would

strike an appropriate balance by protecting consumer personal information processed offshore, without disrupting current business practices.

**4. The requirement that the consumer must consent to the use of the consumer's personal information in certain actuarial studies and research activities would significantly restrict the ability of insurers to conduct necessary insurance functions.**

Section 4(E) places limits on actuarial studies and research, other than those conducted for rating and risk management purposes for the benefit of the licensee using consumers' personal information, by requiring that a licensee obtain a consumer's prior express consent before processing, retaining, or sharing a consumer's personal information in connection with actuarial studies and research. After consumer consent is obtained, Section 4(E)(1) would require that:

- o No consumer can be identified in any research study or report;
- o All materials allowing the consumer to be identified be returned to the licensee that initiated the study; and
- o A consumer's personal information be deleted as soon as the information is no longer needed for the specific actuarial or research study.

These restrictions would provide little benefit to consumers, who are not impacted or inconvenienced by having personal information included in such actuarial studies. But it could significantly impede the ability of licensees to manage and understand their business. It is common practice for insurers to review certain aspects of their business, such as marketing. . This provision, as written, would hamper the ability of licensees to carry out important internal research and review.

No other privacy law restricts any actuarial studies and research by requiring that consumers consent to the use of their data in such studies. By preventing licensees from conducting common product and business research, Section 4(E) of Model #674 would place insurers at a competitive disadvantage when trying to understand their customers and their needs.

The CAI recognizes that any disclosure or sharing of personal information in connection with research does come with some level of increased cybersecurity risk; however, we believe those risks are appropriately addressed through existing NAIC Model Law #668.

CAI Recommendation. Section 4(E) should be revised to allow insurers to use and share consumers' personal data in actuarial studies and research activities for any specified purpose related to insurance, subject to standard obligations for oversight of third party service providers.

**5. The requirements for enhanced third party oversight and contracting requirements would adversely limit the ability of licensees to hire top service providers.**

Section 2 of draft Model #674 would require all third parties that process data in connection with an insurance transaction to be obligated to comply with Model #674 and the licensees own privacy practices. This requirement would appear to function as a long-arm application of Model #674 that service providers would not agree to. Many service providers, such as leading cloud providers, would be unwilling to agree to be subject to compliance with every state's adopted version of Model #674, legislation that would not otherwise apply. Additionally, some service providers would already be subject to GLBA data protections adopted by the SEC or other regulators, and would be unwilling to comply with broader and more stringent insurance specific requirements under Model #674.

For example, insurance company separate accounts investing in underlying mutual funds (UIT separate accounts) necessarily interact with SEC-regulated transfer agents, funds, and investment advisors. It appears that such entities would qualify as service providers of the UIT separate account



under draft Model #674. However, such entities are regulated by the SEC and would likely be unwilling to agree to be subject to the specific requirements of Model #674. If such entities did refuse to adopt the specific contractual obligations required under the Model, the UIT separate account would then be prohibited from continuing to use these SEC-regulated entities. That would then force the UIT separate accounts to attempt to rearrange the entire structure of existing placement and administration of its investments into new and different funds, advisors, and other counterparties, rearrangements that could require SEC approval. This would cause costs and disruption to consumers, while also raising legal and regulatory risks and uncertainties around breach of contract and SEC regulatory requirements.

*CAI Recommendation.* Instead of applying a one-size-fits-all approach that will limit the ability of licensees to engage the best service providers in the market, Model #674 should be revised to take a risk-based approach. The CAI recommends that the Model require licensees to conduct appropriate due diligence and oversight of all third party service providers that process personal information, and require licensees to negotiate appropriate contractual protections based on the assessed risk of the service provider. The Model should not specify what those contractual protections would include beyond limiting the service providers ability to use, share or disclose personal information for purposes other than providing the services.

Additionally, the CAI recommends that the definition of "third party service provider" be revised to exclude affiliates of licensees, and that the Model provide an exemption for the sharing of personal information to entities already subject to Model #674 or the GLBA.

**6. Compliance with the 90-day deletion requirement will not be possible to meet in many circumstances, and the related notice requirement will likely be confusing to consumers.**

Section 5.B. of draft Model #674 requires a licensee to completely delete all of the consumer's personal information within 90 days after the data is no longer necessary to perform any of eight permitted purposes described in Section 5.A. In addition, any third party service provider must notify the licensee when the consumer's information is completely deleted.

The 90-day timeframe for deleting all of a consumer's information in the possession of the insurer is too short and not practical given the number of systems on which a consumer's data may be retained. Personal consumer information can be retained on application, underwriting, operational, claims, marketing and other systems. Some systems may be retired legacy systems that require special programming to delete consumer data, if deletion is even possible. Consumer data can also appear on backup systems that present special issues. Moreover, given the length of time that some personal data must be retained, some consumer data may be on first generation systems where institutional programming knowledge has been lost or the data may even be in paper files that are archived and very difficult to access. In short, the 90-day deadline for deleting data does not reflect the practical challenges of deleting data at an institutional level, and should be revised to take into account the complex realities of record keeping and record deletion across the industry. We also note that the cybersecurity risks associated with retention of personal information is already addressed in Model #668, which requires that a licensee's information security program "define and periodically reevaluate a schedule for retention of Nonpublic Information and a mechanism for its destruction when no longer needed."

Section 5.B also does not address whether it applies retroactively, that is, how this provision will apply to personal consumer information that has been retained for many years beyond the deadlines in this Section.

Finally, Section 5.B. (3) would require a licensee that no longer has a relationship with a consumer in connection with any insurance transactions to send a notice to the consumer that the licensee no longer retains the consumer's personal information. This notice provision is

unprecedented and would be difficult to implement. Moreover, it is likely that a consumer who no longer has a relationship with the licensee will be very confused, and possibly concerned, upon receiving such a notice.

*CAI Recommendation.* Section 5.B. should be revised to allow insurers a reasonable amount of time to delete personal data that is no longer necessary. The Model should not specify a one-size-fits all time period for doing so. Section 5.B. (3) should be deleted in its entirety.

### **7. The notice requirements are too complicated and would dilute their value to consumers.**

While effective and transparent notice is an essential part of consumer privacy protections, the obligations proposed in Model #674 are too broad and would be difficult to meet in practice. The notices would also be hard to understand and not consumer friendly.

Section 6 of the draft Model would create obligations that are impossible to comply with in practice because of the broad definition of a "consumer". As proposed, the Model would require full and annual notification, prior to or at the point of collection, to not only policyholders and annuitants but also claimants, beneficiaries, agents, guardians, and other individuals who do not have a direct relationship with the licensee. In many cases, this will be an impossible standard to meet. For example, it would be impossible for a UIT separate account to provide a privacy notice to the beneficiary of a variable annuity prior to the annuitant actually providing to the UIT separate account the name and other personal information of the beneficiary. Where the licensee does not have a direct relationship with the consumer, licensees cannot know who the consumer is until it has already collected personal information about them.

Additionally, the requirement to provide annual privacy notices to all consumers, even where nothing has changed since the last notice was provided, cuts against the trend in both state law and in federal regulations to reduce the number of annual privacy notices that consumers receive. For example, the SEC is currently proposing amendments to Regulation S-P (which implements GLBA privacy and security requirements) that provides relief from having to provide annual notice where a notice has previously been provided and an entity's privacy practices have not changed. That is consistent with the FAST Act, which was adopted by Congress in 2015 and revised the GLBA annual notice requirement. It is also consistent with the NAIC's own Model Bulletin on GLBA annual privacy notices<sup>5</sup> published in response to the FAST Act, which similarly adopted this more streamlined approach. We suggest that more notice to consumers is not always better. Rather, if consumers receive too many and too frequent privacy notices, it reduces the usefulness and effectiveness of consumer notice in practice.

Section 7 of the draft Model would also require a range of specific disclosure obligations that would be impractical or impossible to meet, while also removing the ability of licensees to be able to use and rely on the federal Model Privacy Form. For example, Section 7.A.(4) would require licensees to identify the specific sources that may be used to collect information about a consumer. However, those sources may not be known for each consumer prior to collecting the data. Additionally, this would suggest that a licensee would be required to update its privacy notices prior to engaging a new vendor to provide consumer data in connection with providing financial products or services.

Similarly, the right under Section 7.A.(6) to obtain a list of the specific persons with which their personal information has been shared in the previous year would be difficult to comply with in practice, while providing little benefit to consumers. As drafted, this notice would be required to cover

---

<sup>5</sup> The *Gramm Leach Bliley Act Annual Privacy Notice NAIC Model Bulletin* is available at [https://content.naic.org/sites/default/files/inline-files/legal\\_bulletin\\_gramm\\_leach\\_bliley\\_act\\_annual\\_privacy\\_notices.pdf](https://content.naic.org/sites/default/files/inline-files/legal_bulletin_gramm_leach_bliley_act_annual_privacy_notices.pdf)

any individual, internal or external, with whom the licensee shared the information. The effort to track each internal individual who helps process requests for services associated with a consumer's annuity, or who helps process a claimant's claim, would be daunting if not impossible in practice, while the benefit to the consumer of receiving such a list is unclear. While this right is similar to an existing right under Section 8.A.(2) of Model #670, that right only applies to the extent the requested information is actually recorded, and otherwise only requires a description of the persons to whom such information is normally disclosed.

Further, for licensees like UIT separate accounts that would be subject to both Model #674 and the SEC's Regulation S-P or other implementations of the GLBA's privacy requirements, Sections 6 and 7 would also subject such licensees to inconsistent and potentially conflicting notice requirements, possibly resulting in two different privacy notices to be sent to the same individuals for the same product.

*CAI Recommendation.* The notice and disclosure requirements in draft Model #674 should be revised to more closely follow the existing notification structure and obligations under Model #672, while appropriately building on those requirements to enhance the quality and transparency of consumer notice. Licensees should also be required to publicly post their privacy notices online and make them available on request, in lieu of having to provide direct notice to individuals that would not currently qualify as customers under Model #672. The overall disclosure obligations should be generalized to allow for practical descriptions and disclosures, such as disclosing the types of sources from which personal information is collected instead of the actual sources. Finally, an updated model form should be developed that would allow licensees to meet the disclosure obligations of Model #674 while also complying with existing requirements for using the Federal Model Form. Doing so would allow licensees to continue to benefit from the safe harbors for using the Federal Model Form while also promoting broader use of consistent and consumer friendly notification practices.

#### **8. The optional private right of action provision should be removed.**

Section 28 of proposed Model #674 would provide an option to state legislatures to include a limited private right of action for any failure to comply with the Model that also violates an individual's rights under the Model. We appreciate that the Working Group has included limitations, such as limiting suits to actual damages and prohibiting class actions. However, this limited private right of action is still ripe for abuse and would subject licensees to litigation related expenses regardless of whether the licensee is fully compliant. Consumers also do not need a private right of action to empower them to thwart inappropriate conduct by a licensee, as consumers are able to file complaints of any violations with state regulators. Regulators already maintain robust complaint intake functions, which are well equipped to identify legitimate issues and ensure licensees appropriately address those issues. Accordingly, enforcement authority for compliance with Model #674 should rest with state regulators.

*CAI Recommendation.* Proposed Section 28 should be revised to remove the option for state legislatures to include a limited private right of action under Subsection B, and instead specify that the law does not create a private right of action using the existing language under Subsection A.

We want to express our deep appreciation for the opportunity to comment on draft Model #674, and we hope that you find these comments helpful at this stage. Please do not hesitate to contact us if you have any questions.

Sincerely,

**For The Committee of Annuity Insurers**

Eversheds Sutherland (US) LLP

By:

A handwritten signature in black ink that reads "Stephen E. Roth". The signature is written in a cursive style and is positioned above a horizontal line.

Stephen E. Roth  
Mary Jane Wilson-Bilik  
Alexander F. L. Sand  
Eversheds Sutherland (US) LLP

April 3, 2023

**VIA ELECTRONIC MAIL – lalexander@naic.org**

NAIC Privacy Protections Working Group  
Chair, Katie Johnson  
National Association of Insurance Commissioners  
c/o Ms. Lois Alexander  
1100 Walnut Street  
Suite 1500  
Kansas City, MO 64106-2197

**RE: Comments on January 31, 2023 Exposure Draft of the Consumer Privacy Protections Model Law (#674)**

Dear Ms. Johnson and members of the Privacy and Protections Working Group:

The Council of Insurance Agents and Brokers (“The Council”) appreciates this opportunity to comment on the working group draft of the Consumer Privacy Protection Model Law.<sup>1</sup> The Council appreciates the efforts to incorporate modernized sections of existing privacy protection models #670 and #672 into a new draft, model #674. Our comments below focus on several of the Council’s key concerns with the NAIC’s draft model. Below we address the following concerns with Model #674:

- Imposing the same direct compliance requirements on all licensees regardless of their role in the cycle of collecting, using, and sharing a consumer’s personal information (PI) does not reflect the operational realities of insurance transactions.
- The requirements for obtaining consumer consent and providing notice fail to account for the burdens on licensees who collect information but have no direct relationship with the consumer.
- The notice requirements regarding third-party collection and the timeframe for deleting and reporting deletion of certain information are unrealistic for our industry.
- The broad scope of these obligations would add unnecessary complexity to the existing web of complex state, cyber, HIPAA, GBLA, global, and potentially, federal privacy requirements.

We look forward to continued discussion with the working group on these important issues.

### **1. Equal Application to All Licensees**

As a general matter, the Council is concerned with the model law’s application of these various obligations to all licensees, with no differentiation between the primary insurance business and the service provider. Other privacy regimes acknowledge the separate roles and responsibilities

---

<sup>1</sup> See NAIC Privacy Protections Working Group Draft: [Exposure Draft Consumer Privacy Protection Model Law #674 01-31-23.pdf](#)

of a business entity on the one hand, and a service provider on the other. This model law applies its requirements equally to any person licensed, authorized to operate, registered, or required to be, pursuant to the insurance laws of the particular state irrespective of whether that person is collecting information on behalf of an insurance entity or receiving information from a commercial entity client with whom the individual has a relationship (e.g., as an employee or claimant.)

## **2. Obtaining Consumer Consent and Providing Notice**

Entities like brokers, that are both licensees and service providers, and who do not necessarily collect PI directly from individuals (but instead, for example, from employers), face an even greater disadvantage under this model law. Brokers would be required to obtain express written consent before any personal information may be used for research or first party marketing (“additional permitted transactions”). However, brokers would have to rely on other entities, such as their clients, to actually obtain the consent from the individual whose information will be collected. Unlike the entity that directly collects the PI and has the opportunity and incentive to collect consent in the manner prescribed for its own needs, indirect recipients of that data (i.e. brokers) would be severely hindered from carrying out their duty to ensure that the deployment of that information is done in a compliant fashion if they are not in a position to obtain the necessary consent.

The same can be said for the obligation to provide notice to consumers. Under the model law, licensees would not be permitted to notify a consumer electronically (either through posting on a site or emailing directly) unless the consumer has agreed to conduct business electronically with the licensee. Notices must be provided to consumers no matter how the receiving licensee has been provided with the personal information, and regardless of whether the recipient has any sort of relationship with the individual. This creates substantial difficulties for insurance transactions that involve multiple parties, such as a placement request containing the names of the insureds submitted to various wholesale brokers, all of whom obtain insurance through a variety of insurers. Under the model law, each of the parties would have been required to send a notice to the individuals before the personal information was collected. As a practical matter, this is not possible, since the retailer is sending the information out to a variety of insurance entities that are not collecting the data directly from the individuals and likely will not have their address. Should each recipient before receiving the information insist on obtaining the individual’s address so that a notice can be sent? This would be untenable in our industry, and would in fact require the collection of additional personal information.

The requirement that consumers provide written consent for offshore processing of data is another key concern, as it represents a major paradigm shift for most US licensees. Many of the Council’s members have globalized business models where they rely on technical operation support abroad for skilled and cost-effective support. Because a single person’s failure to consent at any point could disrupt the entire offshore support model, this written consent obligation is basically a data localization requirement with extensive costs for licensees and no clear benefit. It may also be helpful to note that the NAIC retains its quarterly IID listing of alien insurers, all of whom are located outside of the United States. This new consent requirement would overlay additional regulation upon sending submissions to eligible alien surplus lines insurers, a number of whom are domiciled in the European Union or the United Kingdom, both of which have robust privacy regimes.

Lastly, we are concerned with the varying consent expiration dates for different types of coverage. Under the model law, consumer consent for property and casualty coverage would expire every 90 days and would expire every 2 years for life and health coverage. The administrative burden to maintain compliance with these obligations would be significant and onerous.

The Council suggests a more sensible option that tracks with state and other US privacy laws to instead designate a primarily responsible party who collects the information and provides notice/consent mechanisms to consumers, and an obligation on that responsible party to ensure the data is only shared with additional vetted parties for insurance related and other lawful purposes under contractual restrictions.

### **3. Content of Consumer Notices**

The Council is also concerned with several provisions governing the content of consumer notices. The requirement that licensees be able to provide a list to any individual of any third parties with whom their PI was shared, with a three-year look-back period, would be very difficult to effectuate. Determining whether data was actually shared with a third party for a particular individual, and the necessary maintenance and review of three years' worth of logging or tracking to confirm whether sharing actually took place, is akin to a litigation discovery exercise. In addition, a requirement for licensees to delete PI within 90 days after legal retention obligations have expired compounded with reporting obligations to confirm the deletion, is similarly unrealistic. We therefore suggest removing the three-year look back period and the reporting obligations to confirm PI has been deleted 90 days after legal retention obligations expire.

### **4. Relation to Existing State and Federal Requirements**


Council members are currently subject to a variety of state, federal and global requirements on how consumer information must be handled and their rights with regard to their personal data. Our members must satisfy their obligations under the federal Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach Bliley Act (GLBA), the multitude of state privacy laws, a variety of state data breach notification requirements, and potentially, new federal privacy legislation under consideration. The model law would add another layer to this complex web of privacy requirements that are almost impossible for any one entity to comply with simultaneously.

To further complicate matters, the model law incorporates existing insurance-specific obligations that have no bearing on consumer privacy protection. For example, the model law's inclusion of "adverse underwriting decisions" in a licensee's consumer notification obligations is entirely duplicative of existing requirements under the Fair Credit Reporting Act and deals with underwriting decisions and practices, not consumer privacy.

\* \* \*

Again, we appreciate the working group's continued efforts to update the consumer privacy protections models and your consideration of our comments. Please do not hesitate to contact us if we can provide additional information or answer any questions.

Respectfully submitted,



Joel Kopperud  
Senior Vice President, Government Affairs  
The Council of Insurance Agents & Brokers  
701 Pennsylvania Avenue, NW, Suite 750  
Washington, DC 20004-2608  
(202) 783-4400  
jkopperud@ciab.com



Cari Lee  
Director of State Government Affairs  
The Council of Insurance Agents & Brokers  
701 Pennsylvania Avenue, NW \, Suite 750  
Washington, DC 20004-2608  
608-345-5377  
calee@steptoe.com





April 3, 2023

Ms. Lois Alexander  
Market Regulation Manager  
National Association of Insurance Commissioners  
1100 Walnut Street, Suite 1500  
Kansas City, MO 64106-2197

Dear Ms. Alexander:

The Global Data Alliance (GDA)<sup>1</sup> respectfully submits comments to the National Association of Insurance Commissioners (NAIC) on the initial exposure draft of the Insurance Consumer Privacy Protection Model Law #674 (“Model Law 674”). The GDA appreciates this comment opportunity.

The GDA has serious concerns regarding the breadth of the Model Law’s restrictions on cross-border data transfers – restrictions that are at odds with prevailing domestic and international cross-border data legal norms, including US international legal obligations under international treaties, agreements, and other commitments.

We strongly urge the NAIC to remove these limitations from the Model Law pending a more thorough review of their economic and legal implications. We also urge NAIC to assess the necessity of exclusive reliance on the consent-based restrictions on data transfers, and to consider alternative approaches that would be less restrictive of data transfers and that would not raise the same risks. Finally, the GDA would welcome a virtual meeting with NAIC staff.

## **I. About the Global Data Alliance**

The GDA is a cross-industry coalition of companies that support millions of jobs across the United States. The GDA represents companies that are committed to high standards of data responsibility, privacy, and security, and that rely on the ability to transfer data around the world to innovate and create jobs.

The GDA works to advance policies that promote the responsible handling of data without imposing unnecessary data localization mandates or restrictions on data transfers. The GDA focuses on cross-border data policy proposals across 60+ jurisdictions, across sectoral regulations, and across legal disciplines, including artificial intelligence, consumer protection, cybersecurity, international trade, law enforcement access to data, privacy and personal data protection, and other matters. The GDA has a strong interest in promoting coherent and interoperable legal frameworks that help instill trust in the digital economy while safeguarding the ability to transfer data across borders.

Alliance members are active across many sectors including the agriculture,<sup>2</sup> automotive,<sup>3</sup> clean energy,<sup>4</sup> finance and insurance,<sup>5</sup> healthcare and medical technology,<sup>6</sup> logistics,<sup>7</sup> media,<sup>8</sup> pharmaceutical,<sup>9</sup> and telecommunications sectors.<sup>10</sup> The Global Data Alliance develops studies and reports, as well as model legal texts, on the cross-border aspects of data privacy, cybersecurity, and other legislative or regulatory proposals. This includes the [GDA Cross-Border Data Policy Principles](#).<sup>11</sup>

The ability to transfer data in a trusted and secure manner across transnational digital networks is of central importance to the national policy objectives of many countries, including the United States. Data transfers support cybersecurity,<sup>12</sup> fraud prevention,<sup>13</sup> and other activities relating to the protection of health, privacy, security, safety, consumers, and the environment. They also support shared economic prosperity:<sup>14</sup> Cross-border access to marketplaces, purchasers, suppliers, and other commercial partners allows U.S. enterprises of all sizes and in all sectors<sup>15</sup> to engage in mutually beneficial international transactions with foreign enterprises. 75 percent of the value of data transfers accrues to companies in sectors such as manufacturing, agriculture, and logistics<sup>16</sup> and at every stage of the value chain.<sup>17</sup> Finally, scientific and technological progress require the exchange of information and ideas across borders<sup>18</sup>: As the WTO has stated, “for data to flourish as an input to innovation, it benefits from flowing as freely as possible.”<sup>19</sup>

## II. Legal Background

The GDA has reviewed Model Law 674 with interest and care. The GDA supports the efforts of the NAIC to improve consumer privacy in insurance markets through the Model Law. As an organization focused on cross-border data policy issues, the GDA limits its comments to aspects of the Model Law that relate to international data transfers. Please refer to the comments of other organizations regarding aspects of the Model Law that do not relate to international data transfers.

The GDA focuses its comments on the following sections of the Model Law (emphasis added).

### Section 4 – A 5(b)

No licensee shall collect, process, retain, or share a consumer’s personal information unless:

The licensee or third-party service provider has obtained prior consent from any consumer whose personal information will be:

Shared with a person outside the jurisdiction of the United States, or its territories, as provided in this Act.

**(C)** No licensee shall, unless legally required, collect, process, retain, or share a consumer’s personal information with an entity outside of the United States and its territories, unless the licensee has provided the required notice and obtained the consumer’s prior express consent to do so, as required by Article III of this Act.

### Section 7 – 7(a)

The requirement that the licensee or third-party service provider obtain the consumer’s express written consent prior to sharing the consumer’s personal information with any person in connection with the collection, processing, retention, or sharing of the consumer’s personal information with a person in a jurisdiction outside of the United States and its territories, and the consumer’s right to prohibit sharing of the consumer’s personal information with such a person;

(C)

(1) A statement that the consumer may, but is not required to, consent to the collection, processing, retention, or sharing, of the consumer’s personal information a jurisdiction outside of the United States and its territories;

(3) That once consent has been given for the collection, processing, retention, or sharing of consumers' personal information in a jurisdiction outside the United States and its territories, a consumer may revoke consent at any time; and

(4) That once consent for the collection, processing, retention, or sharing of consumers' personal information by a person in a jurisdiction outside the United States and its territories has been revoked, any of the consumer's personal information in the possession of such person shall be deleted as set forth in Section 5 of this Act

Section 19 – A (1)(b)

The licensee obtains all necessary consent of consumers' whose personal information is shared with a person outside the jurisdiction of the United States or its territories, as provided in this Act; and

### III. Discussion

As drafted, the initial exposure draft would limit data transfers outside of the United States exclusively on the basis of data subject consent. This limitation is at odds with prevailing domestic and international cross-border data legal norms, including US international legal obligations.

We strongly urge the NAIC to remove these limitations from Model Law 674, pending further review of their legal and economic implications and consultation with the Federal Government. We also urge NAIC to fully assess the necessity of the consent-based restrictions on data transfers, and to consider alternative approaches that would be less restrictive of data transfers and that would not raise the same economic and legal risks.

Broadly speaking, permitting cross-border data transfers solely on the basis of consent is far outside of prevailing international norms and best practices in relation to cross-border data policy. Advancing a rule that premises data transfers exclusively upon consent – without any other bases for processing or transfer – would render the Model Law as one of the most restrictive cross-border data transfer measures, if not the most restrictive such measure in the world.

First, we urge the NAIC to consider state-level privacy legislation being advanced across the United States. The data transfer restrictions of the Model Law are at odds with all US state privacy laws in effect today. None of the existing state laws (California, Colorado, Connecticut, Iowa, Utah or Virginia) contain the type of cross-border data restriction that Model Law 674 proposes to implement. These and other states have not adopted such restrictions for good reason: Far from advancing privacy objectives,<sup>20</sup> such restrictions frequently hurt small businesses;<sup>21</sup> undermine data security and cybersecurity;<sup>22</sup> threaten human rights;<sup>23</sup> slow scientific progress and innovation;<sup>24</sup> and impair various safety, health,<sup>25</sup> environmental protection,<sup>26</sup> and other state and national policy priorities.<sup>27</sup>

Second, we also urge the NAIC to account for, and accord due legal respect to, the Foreign Affairs power of the US federal government under Article 1 of the US Constitution, as affirmed in Supreme Court jurisprudence such as *Crosby v. National Foreign Trade Council* and *American Insurance Association v. Garamendi*.<sup>28</sup> The data transfer provisions of Model Law 674 raise questions of consistency with numerous existing treaties, international agreements, Presidential and other official acts of the United States – some of which that the NAIC provided explicit consent to the Office of the United States Trade Representative (USTR) to negotiate, and was afforded

the opportunity to review during the negotiations. These existing instruments and acts include the cross-border data transfer and data localization commitments adopted by the United States in: (1) its Free Trade Agreements and Digital Economy Agreements (such as the US-Mexico-Canada Agreement),<sup>29</sup> (2) at the World Trade Organization,<sup>30</sup> (3) at the Group of 7,<sup>31</sup> (4) at the Group of 20,<sup>32</sup> and (5) in US Department of Treasury financial regulatory dialogues with foreign counterparts.<sup>33</sup> The position put forward in the exposure draft is also at odds with positions taken by global regulatory bodies such as the Financial Stability Board and the International Organization of Securities Commissions (“IOSCO”).

Third, the cross-border data transfer restrictions in the exposure draft of Model Law 674 are also in tension with broader international privacy and cross-border data policy trends. Such restrictions are contrary to the positions adopted by US peer countries such as the EU, UK, Singapore, Japan, and Australia. These governments support the free flow of data, including for personal information, and the need to prohibit data localization requirements, while at the same time maintaining privacy frameworks. For example, the EU’s General Data Protection Law (GDPR) permits data transfers on numerous grounds beyond the consent of data subjects.<sup>34</sup>

In lieu of the approach outlined in Model Law 674, the EU and other countries have adopted an approach modeled on the so-called “accountability principle,” which reflects the prevailing international legal norm relating to the cross-border transfer of data.<sup>35</sup> Under this principle, organizations that transfer data globally should implement procedures to ensure that data will continue to be protected, even if it is transferred to countries other than where it was first collected. The accountability principle was first developed by the OECD,<sup>36</sup> and was subsequently endorsed and has been integrated in many legal systems including the EU,<sup>37</sup> Japan,<sup>38</sup> New Zealand,<sup>39</sup> Singapore,<sup>40</sup> and Canada.<sup>41</sup> This principle is also a significant feature of the APEC Privacy Framework,<sup>42</sup> the APEC Privacy Recognition for Processors (PRP) system,<sup>43</sup> the APEC Cross Border Privacy Rules (CBPR) system,<sup>44</sup> and the ASEAN Model Contractual Clauses.<sup>45</sup>

Finally, notwithstanding the GDA’s concerns regarding the foregoing aspects of Model Law 674, we wish to underscore that the GDA strongly supports NAIC’s goals to protecting consumer information and privacy and personal data protection. GDA members adhere to high standards of data responsibility, data privacy, and data security. However, privacy, data protection, and data security are not dependent on the location of data storage or processing, or the location of the infrastructure supporting it. Rather, protection is a function of the manner in which personal data is protected. What matters most is not where such data is, but rather how it is protected, as embodied in the technologies, systems and internal controls put in to place to protect it.

We urge the NAIC to remove the above-referenced cross-border data restrictions that are at odds with domestic and international legal standards and best practices.

Respectfully yours,

*Joseph Whitlock*

Joseph P. Whitlock  
Executive Director  
Global Data Alliance

- <sup>1</sup> The Global Data Alliance produces draft treaty and legal texts, regulatory analysis, and sector- and issue-focused studies on cross-border data and digital trust. For more information, please visit the GDA website, at: [www.globaldataalliance.org](http://www.globaldataalliance.org)
- <sup>2</sup> Global Data Alliance, *GDA Website – Agriculture* (2022), at: <https://globaldataalliance.org/sectors/agriculture/>
- <sup>3</sup> Global Data Alliance, *GDA Website – Automotive* (2022), at: <https://globaldataalliance.org/sectors/automotive/>
- <sup>4</sup> Global Data Alliance, *GDA Website – Energy* (2022), at: <https://globaldataalliance.org/sectors/energy/>
- <sup>5</sup> Global Data Alliance, *GDA Website – Finance* (2022), <https://globaldataalliance.org/sectors/finance/>
- <sup>6</sup> Global Data Alliance, *GDA Website – Healthcare* (2022), <https://globaldataalliance.org/sectors/healthcare/>
- <sup>7</sup> Global Data Alliance, *GDA Website – Supply Chain Logistics* (2022), <https://globaldataalliance.org/sectors/supply-chain-logistics/>
- <sup>8</sup> Global Data Alliance, *GDA Website – Media and Publishing* (2022), <https://globaldataalliance.org/sectors/media-publishing/>
- <sup>9</sup> Global Data Alliance, *GDA Website – Biopharmaceutical R&D* (2022), <https://globaldataalliance.org/sectors/biopharmaceutical-rd/>
- <sup>10</sup> Global Data Alliance, *GDA Website – Telecommunications* (2022), <https://globaldataalliance.org/sectors/telecommunications/>
- <sup>11</sup> Global Data Alliance, *Cross-Border Data Policy Principles* (2021), <https://globaldataalliance.org/wp-content/uploads/2021/07/03022021gdacrossborderdatapolicyprinciples.pdf>
- <sup>12</sup> Global Data Alliance, *Cross-Border Data Transfers & Data Localization Measures* (2020), <https://globaldataalliance.org/wp-content/uploads/2021/07/02112020GDACrossborderdata.pdf>
- <sup>13</sup> Global Data Alliance, *GDA Website – Finance* (2022), <https://globaldataalliance.org/sectors/finance/>
- <sup>14</sup> Global Data Alliance, *Cross-Border Data Transfers & Economic Development: Access to Global Markets, Innovation, Finance, Food, and Healthcare* (2021), <https://globaldataalliance.org/wp-content/uploads/2021/07/05062021econdevelopments1.pdf>
- <sup>15</sup> Global Data Alliance, *The Cross-Border Movement of Data: Creating Jobs and Trust Across Borders in Every Sector* (2020), <https://globaldataalliance.org/wp-content/uploads/2021/07/GDAeverysector.pdf>
- <sup>16</sup> Global Data Alliance, *Cross-Border Data Transfer Facts and Figures* (2020), <https://globaldataalliance.org/wp-content/uploads/2021/07/gdafactsandfigures.pdf>
- <sup>17</sup> Global Data Alliance, *Global Data Alliance Infographic: Jobs in All Sectors Depend Upon Data Flows* (2021), <https://globaldataalliance.org/wp-content/uploads/2021/07/infographicgda.pdf>
- <sup>18</sup> Global Data Alliance, *Cross-Border Data Transfers & Innovation* (2020), <https://globaldataalliance.org/wp-content/uploads/2021/07/04012021cbdtinnovation.pdf>
- <sup>19</sup> WTO, *Government Policies to Promote Innovation in the Digital Age*, 2020 World Trade Report (2020), at: [https://www.wto.org/english/res\\_e/booksp\\_e/wtr20\\_e/wtr20-0\\_e.pdf](https://www.wto.org/english/res_e/booksp_e/wtr20_e/wtr20-0_e.pdf)
- <sup>20</sup> Global Data Alliance, *Cross-Border Data Transfers & Privacy* (2023), at: <https://globaldataalliance.org/issues/privacy/>
- <sup>21</sup> Global Data Alliance, *Cross-Border Data Transfers & Small Businesses* (2023), at: <https://globaldataalliance.org/issues/small-businesses/>
- <sup>22</sup> Global Data Alliance, *Cross-Border Data Transfers & Cybersecurity* (2023), at: <https://globaldataalliance.org/issues/cybersecurity/>
- <sup>23</sup> Freedom House, *Countering an Authoritarian Overhaul of the Internet* (2022), at: <https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet> Freedom House explains the nexus between data transfer restrictions and human rights abuse as follows (emphasis added):

“In at least 23 countries covered by Freedom the Net, laws that limit where and how personal data can flow were proposed or passed during the coverage period. ... The transfer of data across jurisdictions is central to the functioning of the global internet and benefits ordinary users, including by improving internet speeds, enabling companies to provide critical services worldwide, and allowing the storage of records in the most secure data centers available.

As policymakers impose necessary privacy laws that safeguard sensitive information from commercial abuse, they may unintentionally drive fragmentation by creating a barrier between their own countries and those without similar standards. The ensuing patchwork of regulations could incentivize companies, particularly newer or smaller services, to concentrate their growth in certain countries, resulting in less diverse online ecosystems for users elsewhere. ...

[S]ome [countries] have buried problematic obligations that either mandate domestic data storage, feature blanket exceptions for national security or state actors without safeguards, or delegate increased decision-making power to politicized regulators—all of which renders users vulnerable to government abuse despite

improvements pertaining to the use of personal data for commercial purposes. Such contradictory “data washing” measures ultimately fail to strengthen privacy and further fragment the internet....”

<sup>24</sup> Global Data Alliance, *Cross-Border Data Transfers & Innovation* (2023), at:

<https://globaldataalliance.org/issues/innovation/>

<sup>25</sup> Global Data Alliance, *Cross-Border Data Transfers & Biopharmaceutical R&D* (2022), at

<https://globaldataalliance.org/sectors/biopharmaceutical-rd/>; Global Data Alliance, *Cross-Border Data Transfers & Medical Technology* (2023), at: <https://globaldataalliance.org/sectors/medical-technology/>; Global Data Alliance, *Cross-Border Data Transfers & Healthcare* (2022), at:

<https://globaldataalliance.org/sectors/healthcare/>

<sup>26</sup> Global Data Alliance, *Cross-Border Data Transfers & Environmental Sustainability* (2023), at:

<https://globaldataalliance.org/issues/environmental-sustainability/>

<sup>27</sup> Global Data Alliance, *Cross-Border Data Transfers & Regulatory Compliance* (2023), at:

<https://globaldataalliance.org/issues/regulatory-compliance/>

<sup>28</sup> See generally, Congressional Research Service, *Constitutional Limits on States’ Power over Foreign Affairs* (Aug. 15, 2022), at: <https://crsreports.congress.gov/product/pdf/LSB/LSB10808>; See also, Supreme Court of the United States, *Crosby v. National Foreign Trade Council*, 530 U.S. 363 (2000), at:

<https://tile.loc.gov/storage-services/service/ll/usrep/usrep530/usrep530363/usrep530363.pdf>; Supreme Court of the United States, *American Insurance Association v. Garamendi*, 539 US 396 (2003), at:

<https://tile.loc.gov/storage-services/service/ll/usrep/usrep539/usrep539396/usrep539396.pdf>

<sup>29</sup> See generally, US-Mexico-Canada Agreement, Art. 19.11-19.12; 17.17-18, at: <https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between>; US-Japan Digital Trade Agreement, Arts. 11-13, at:

[https://ustr.gov/sites/default/files/files/agreements/japan/Agreement\\_between\\_the\\_United\\_States\\_and\\_Japan\\_concerning\\_Digital\\_Trade.pdf](https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf)

<sup>30</sup> See WTO General Agreement on Trade in Services (1995), at:

[https://www.wto.org/english/tratop\\_e/serv\\_e/gsintr\\_e.pdf#:~:text=The%20General%20Agreement%20on%20Trade%20in%20Services%20%28GATS%29,of%201947%2C%20the%20GATS%27%20counterpart%20in%20merchandise%20trade](https://www.wto.org/english/tratop_e/serv_e/gsintr_e.pdf#:~:text=The%20General%20Agreement%20on%20Trade%20in%20Services%20%28GATS%29,of%201947%2C%20the%20GATS%27%20counterpart%20in%20merchandise%20trade)

<sup>31</sup> See e.g., G7 Trade Ministers’ Statement (Sept. 15, 2022), at: <https://ustr.gov/sites/default/files/2022-09/G7%20Trade%20Ministers'%20Statement%202022.pdf>; G7 Data Protection and Privacy Authorities’

Communique (Sept. 8, 2022), at: [https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Kurzmeldungen/G7-Communique.pdf?\\_\\_blob=publicationFile&v=3](https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Kurzmeldungen/G7-Communique.pdf?__blob=publicationFile&v=3)

<sup>32</sup> [G20 Osaka Leaders’ Declaration | Documents and Materials | G20 Osaka Summit 2019 \(mofa.go.jp\)](https://www.g20.org/declaration)

<sup>33</sup> See e.g., United States-Singapore Joint Statement on Financial Services Data Connectivity (Feb. 6, 2020),

at: <https://www.mas.gov.sg/news/media-releases/2020/united-states-singapore-joint-statement-on-financial-services-data-connectivity>

<sup>34</sup> See generally, GDPR Chapter V, including Articles 45-46.

<sup>35</sup> The GDA strongly supports the accountability model for international data transfers. This model was, first established by the OECD and subsequently endorsed and integrated in many legal systems and privacy principles. The accountability model provides an approach to cross-border data governance that effectively protects the privacy and consumer rights of individuals and fosters streamlined, robust data flows by requiring entities that collect personal information (often defined as personal data controllers) to be responsible for its protection no matter where or by whom it is processed.

While governments are rightfully concerned with risks to privacy and data security, these risks are not dependent on the physical location of where data is stored or processed, or the location of the infrastructure supporting it. In fact, the effectiveness of data security and personal information protection is a function of the technologies, systems, and procedures put in place by the companies handling the personal information to protect the data.

To benefit from cross-border data transfers while simultaneously ensuring the responsible processing and protection of data, the focus of privacy policy and regulation needs to be on the quality and effectiveness of the mechanisms and the controls maintained to protect the data in question. The accountability model, therefore, continues to be an important tool in increasing privacy and security by requiring entities to ensure that data will continue to be properly protected, regardless of where the data is located.

Personal data protection and privacy frameworks that are based on a common set of international consensus-based principles facilitate cross border data transfers and drive innovation and business investment in local markets by promoting international interoperable legal frameworks upon which businesses of all sizes can rely.

---

These coordination mechanisms also help to bridge current gaps in international privacy norms while facilitating the safe and secure international transfer of personal information. Such mechanisms may include private codes of conduct, contractual arrangements such as standard contractual clauses, certifications such as the APEC Cross Border Privacy Rules (CBPR), seals or marks, and mutual recognition arrangements such as the adequacy with the European Union General Data Protection Regulation (GDPR).

<sup>36</sup> OECD Privacy Framework 2013 (p15), [http://www.oecd.org/sti/ieconomy/oecd\\_privacy\\_framework.pdf](http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf)

<sup>37</sup> Directive 95/46/EC (General Data Protection Regulation), <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

<sup>38</sup> Act on the Protection of Personal Information, <https://www.ppc.go.jp/en/legal/>

<sup>39</sup> Privacy Act 2020, <https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html>

<sup>40</sup> Personal Data Protection Act 2012, <https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act>

<sup>41</sup> *Personal Information Protection and Electronic Documents Act*, Fair Information Principles, [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p\\_principle/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/)

<sup>42</sup> *APEC Privacy Framework*, [https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-\(2015\)](https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015))

<sup>43</sup> *APEC Privacy Recognition for Processors*, at: <https://www.pdpc.gov.sg/help-and-resources/2021/10/apec-cross-border-privacy-rules-and-privacy-recognition-for-processors-systems>

<sup>44</sup> *APEC Cross Border Privacy Rules system*, at: <https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System>

<sup>45</sup> *ASEAN Model Contractual Clauses* (2021), at: [https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows\\_Final.pdf](https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf); See also, Singapore Personal Data Protection Commission, *Guidance for Use of ASEAN Model Contractual Clauses for Cross-Border Data Flows in Singapore* (2022), at: <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Singapore-Guidance-for-Use-of-ASEAN-MCCs.pdf?la=en#:~:text=The%20ASEAN%20Model%20Contractual%20Clauses%20%28ASEAN%20MCCs%29%20are,parties%20that%20protects%20the%20data%20of%20data%20subjects.>

# Arbor Strategies, LLC

**Chris Petersen**  
804-916-1728  
[cpetersen@arborstrategies.com](mailto:cpetersen@arborstrategies.com)

April 3, 2023

Ms. Katie Johnson  
Chair, NAIC Privacy Protections (D) Working Group  
Bureau of Insurance  
Tyler Building  
1300 East Main Street  
Richmond, VA 23210

Dear Ms. Johnson:

I am writing on behalf of a Coalition<sup>1</sup> of health insurers representing some of the country's largest major medical insurers and health maintenance organizations to comment on the NAIC's draft Insurance Consumer Privacy Protection Model Law #674 ("Draft Model 674"). We offer the following general observations that are critical to the development of any privacy policy model:

1. Any new model should include a properly drafted HIPAA safe harbor to reflect the reality that a robust regulatory framework already exists for HIPAA-protected data;
2. Any language regarding a private cause of action is inappropriate in any new NAIC privacy model; and
3. Restrictions on data localization and/or cross-border data provisions conflict with federal laws and treaties and should be removed; and
4. Changes to the privacy rules must be done cautiously and carefully to ensure compliance and avoid consumer and insurer confusion.

---

<sup>1</sup> CVS Health/Aetna, Elevance/Anthem, Cigna and UnitedHealthcare, who together provide health insurance and health maintenance organization coverage to more than 200 million members nationwide, are the members of this Coalition.



## **A Properly Drafted HIPAA Safe Harbor is Essential**

A HIPAA safe harbor ensures that there is a strong national standard that is consistently applied and enforced on HIPAA-covered entities and other parties complying with the HIPAA privacy rule. It also provides uniformity and administrative efficiencies for insurers and medical providers and creates certainty for consumers and insurers. Fortunately, Draft Model 674 includes a safe harbor; however, we recommend that the safe harbor be amended in two key areas. First, as provided in Model 672, the safe harbor should apply to any licensee that complies with the HIPAA privacy rule standards. Second, the scope of the safe harbor should be expanded to include the entire model or at least those provisions that are also regulated under the HIPAA privacy rule.

The safe harbor language from Model 672 works, and it should be retained. Model 672 provides that “[I]rrespective of whether a licensee is subject to the federal Health Insurance Portability and Accountability Act privacy rule as promulgated by the U.S. Department of Health and Human Services [insert cite] (the “federal rule”), if a licensee complies with all requirements of the federal rule except for its effective date provision, the licensee shall not be subject to the provisions of this Article V.”<sup>2</sup> This language has already been vetted and approved by the NAIC. In addition, a significant number of states have also already adopted safe harbor language based on Model 672 language.

This approach allows insurance departments to assert jurisdiction over any insurer they determine is not complying with HIPAA. Thus, there is a lack of state enforcement capacity related to HIPAA-covered entities. It also provides for consistent enterprise compliance and consumer expectations.

The safe harbor should apply to all of the Model Act's provisions covered by the HIPAA privacy rule. As presently drafted, Draft Model 674 creates inconsistencies with HIPAA in key areas, which will cause significant inconsistencies in application and enforcement. It also limits the HIPAA safe harbor to Sections 4-8 of Draft Model 674, even though HIPAA regulates all of the significant subject areas of the proposed model. The HIPAA privacy rule also regulates the following provisions of Draft Model 674:

- Section 2. Oversight of Third-Party Service Provider Arrangements;<sup>3</sup>
- Section 9. Consumer Consent-How Obtained;<sup>4</sup>
- Section 10. Content of Authorizations;<sup>5</sup>
- Section 11. Access to Personal Information;<sup>6</sup>
- Section 12. Correction or Amendment of Personal Information<sup>7</sup>; and

---

<sup>2</sup> Model 672, §21.

<sup>3</sup> 45 CFR §164.308(b)(1)-(3). *See also* 45 CFR §§164.314(a) and 164.504(e)(1)

<sup>4</sup> *Id.* at §164.152

<sup>5</sup> *Id.* at §164.508(b) and (c)

<sup>6</sup> *Id.* at §164.524

<sup>7</sup> *Id.*

Section 13 Nondiscrimination and Nonretaliation<sup>8</sup>

Congress clearly stated when it enacted HIPAA that it has supremacy over any conflicting state statute. Accordingly, the HIPAA privacy rule preempts state laws that do not meet HIPAA standards, and states may not enforce provisions that are contrary to the HIPAA privacy rules. Expanding the scope of the safe harbor to all provisions that are covered under the HIPAA privacy rule avoids duplication and confusion and enhances compliance. It will also free health plans from conducting unnecessary, and costly preemption analyses on a state-by-state basis.

Based upon the above, we recommend that Section 19 of the Draft Model 674 be deleted and replaced with the following language, which is based on NAIC Model 672's safe harbor:

Section 19. Relationship with Federal Laws

Irrespective of whether a licensee is subject to the federal Health Insurance Portability and Accountability Act privacy rule as promulgated by the U.S. Department of Health and Human Services [insert cite] (the "federal rule"), if a licensee is compliant with all requirements of the federal rule except for its effective date provision, and the Health Information Technology For Economic and Clinical Health Public Act and the nondiscrimination provisions of the Affordable Care Act and the rules issued thereunder and shares all personal information in the same manner as protected health information, the licensee shall be deemed to comply with Sections 2-13 of this Act.

While conducting our review of Draft Model 674, it became clear that several of the proposed optional provisions, which were taken from existing models, are either obsolete or not applicable to regulation of privacy. We recommend that the Working Group delete Sections 14-18 from Draft Model 674.

**The Model Should Not Include a Private Cause of Action**

Subsection 28(B) of Draft Model 674 would, if adopted, create a private cause of action. Our coalition of companies strongly oppose including a private cause of action in the model act. The legislative history of Model 670 clearly shows that a private cause of action does not enjoy sufficient state support to be included in a model act. Only a few states have a private cause of action, and where it was adopted, it is very limited. States have had over 40 years to consider including a private right of action, which has been resoundingly rejected. The new proposed privacy model should be a consensus document. Clearly, a private cause of action is not a consensus position, and, as a result, optional Subsection B in Section 28 should be deleted.

---

<sup>8</sup> 45 CFR §160.316

### **Limitation on Off-Shore Data Sharing Is Inappropriate**

Section 4 of Draft Model 674 states that licensees must provide consent prior to sharing covered information with “a person outside the jurisdiction of the United States, or its territories, as provided in this Act.” Other provisions of Draft Model 674 also appear to regulate the sharing of information outside the jurisdiction of the United States. This language would appear to conflict with HIPAA, other federal laws, and international legal obligations. Federal law already sets out the legal landscape in these issue areas. HIPAA does not place any restrictions on this type of sharing so long as proper business associate agreements are in place. This provision, which requires consumer consent, creates barriers to care for health insurers covering consumers outside of the U.S. or those with operations outside the U.S in conflict with international policy and federal laws .

This model stands in stark contrast to global best practices on cross-border data legal frameworks, permitting the free flow of data across borders. The proposed model notes that the model is not intended to supersede federal law, but despite this statement, this model appears to do so in this area. In particular, the model violates various provisions of recent free trade agreements including the U.S.-Mexico-Canada Agreement and the U.S.-Japan Digital Trade Agreement.<sup>9</sup> Provisions include legally binding commitments to prohibit data localization requirements and restrictions on cross-border data flows for financial service suppliers, including inter alia all insurance and insurance-related services. The NAIC was consulted during the negotiation of these trade agreements by the Federal Government and gave their affirmative consent to United States trade representative to negotiate these provisions on behalf of the 56 members of the NAIC. This could raise constitutional issues regarding the ability of state law to interfere with federal treaties and the Foreign Affairs power of the United States federal government under Article 1 of the U.S. Constitution.

The ability to transfer data and access personal information across borders is essential to insurers of all sizes. Flows of data are as important to the global economy today as is the flow of goods, services, and capital and can be vital to the interests of globally mobile consumers, in particular with respect to health care delivery and administration. Consequently we ask that Section 4, Subsection A, Subparagraph 5(b), those provisions in Section 7 that reference jurisdiction outside the United States, and Section 19, Subsection A, Subparagraph (1)(b) be stricken from Draft Model 674.

---

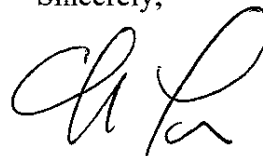
<sup>9</sup> *See for example* AGREEMENT BETWEEN THE UNITED STATES OF AMERICA AND JAPAN CONCERNING DIGITAL TRADE at Article 11 Cross-Border Transfer of Information by Electronic Means “Neither Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means, if this activity is for the conduct of the business of a covered person.” *See also* USMCA Article 17.6: Cross-Border Trade Standstill No Party shall adopt a measure restricting any type of cross-border trade in financial services by cross-border financial service suppliers of another Party that the Party permitted on January 1, 1994, or that is inconsistent with Article 17.3.3 (National Treatment), with respect to the supply of those services.

**Changes to the Privacy Rules Must be Done Cautiously and Carefully.**

Finally, as we noted in earlier comment letters, the United States Department of Health and Human Services (“HHS”) cautions that changes to privacy laws must be done cautiously and carefully. In the executive summary of its June 2021 proposed modifications to the HIPAA privacy rule, the HHS specifically warns that when done improperly, privacy rules “could present barriers to coordinated care and case management—or impose other regulatory burdens without sufficiently compensating for, or offsetting, such burdens through privacy protections.”<sup>10</sup> HHS also warns that the unintended consequences of privacy rules that fail to consider all of the nuances of our health care system could “impede the transformation of the health care system from a system that pays for procedures and services to a system of value-based health care that pays for quality care.”<sup>11</sup> The same caution should be applied to any changes to the NAIC privacy model.

Thank you for allowing us to comment. If you have any questions, please feel free to reach out to me at either (202) 247-0316 or [cpetersen@arborstrategies.com](mailto:cpetersen@arborstrategies.com). We look forward to working with the Working Group as it continues to draft revisions to Draft Model 674.

Sincerely,



Chris Petersen

cc: Lois Alexander

---

<sup>10</sup> Federal Register, Vol. 86, No.12, Thursday, January 21, 2021 at page 6447

<sup>11</sup> *Id.*

March 20, 2023

David Buono  
Office of Market Regulation  
Insurance Department  
1345 Strawberry Square  
Harrisburg, PA, 17120

Dear Dave,

**RE: NAIC Insurance Consumer Privacy Protection Model Law #674**

On behalf of the Insurance Agents & Brokers of Pennsylvania, I am writing to submit some preliminary comments on the NAIC Insurance Consumer Privacy Protection Model Law. We appreciate the opportunity to share our initial reactions ahead of your meeting.

To be perfectly frank, IA&B has serious issues with this draft. IA&B has long had concerns over privacy laws and regulations gradually blurring the lines and eroding common-law rights of independent agents. This NAIC model #674 could put these threats into statutory form. The model also seems to curtail some of the fundamental roles expected of and performed by insurance producers, as defined in the states' Producer Licensing statutes. Some of the issues may stem from the fact that the definition of "licensee" includes both insurers and producers, and the breadth of some of the obligations.

More specifically:

First and foremost, Model #674 **infringes on independent agents' common-law rights to *ownership of expirations***, which is the cornerstone of the American Agency System and which applies to *independent agents*. This ownership is the main asset of any independent agency (see excerpt below from Matthew Bender publication on insurance laws). When examining an agency contract, it is the most important provision that an agent must consider to ensure that his/her rights under law are not undermined by the contract.

*"§ 8.05 Ownership of Records; Expiration Lists (Excerpt from Matthew Bender)*

*The pivotal aspect is that the agent, under the system, owns the agency records in principle because his or her effort and expense generated the business. Accordingly, the expiration lists and insurance records of the agency belong to the agency and not to the insurer. As a corollary, an attribute of the American agency system, is that the insurer, terminating an agent, will not use its own knowledge of the accounts and the expirations to induce the insured to change agents.*

*So fundamental is the ownership of the expiration lists that at one time the American agency system was deemed to be just that.*

*Today, however, the doctrine generally characterizes the independent contractor-agent relationship to an insurer as contrasted to employed field personnel, insurer-owned agencies, and the like.”*

The model also seems to negate, to a great extent, the concept of **work product**, ubiquitous in business, by asking producers to relinquish control over that work product, if the consumer so chooses. In insurance, and specifically in underwriting, information collected in connection with the application process becomes part of the agency’s work product.

As worded, Model #674 would also limit *all* insurance producers’ ability to retain and use, for **solicitation purposes**, information collected through their effort. An insurance producer license is what permits an individual and entity to “sell, solicit and negotiate” insurance under state statutes. The model considerably weakens the term “solicit” by requiring agencies to secure a separate consumer consent before conducting any “additional permitted transaction,” including marketing. An insurance producer’s ability to solicit and “market” other products than that which the consumer initially requested should not be curtailed in any way, including through an additional consent. A producer must be able to suggest a personal umbrella or a flood insurance policy, newly available coverages or higher limits. We would argue that insurance regulators themselves expect producers to do so.

While we would not dispute that regulators’ concern is well intentioned, we would like to understand why the NAIC is choosing to add a completely new law to an already extensive library of federal and state privacy laws and regulations, particularly considering the significant overlap between them. We really see no need for a new privacy model, particularly this radical, and would not be in a position to support it.

- It seems that some of the requirements may be targeted at providing more transparency on underwriting criteria and/or the reasons behind underwriting decisions. We believe that provisions that may seek to better assess rating mechanisms should 1) remain separate from the privacy model and 2) exclude insurance producers from their scope. The rating process is an insurer rather than a licensee issue. Therefore, we would suggest differentiating the applicability by segregating these sections dealing with *incoming* information and underwriting decisions from those dealing with *outgoing* information sharing.
- By nature, independent insurance agents are protective of their customers’ information. They understand existing privacy laws and regulations, and also need to protect their own book of business. This protection of their book is the reason why so many agencies utilize non-compete and/or non-piracy/non-solicitation agreements with their employees and settle the matter in court over indiscretions on the part of former employees who try to steer customers to their new employer.

The model in our view has several fundamental issues:

- We are unclear how our members can properly comply with the interaction of and possible conflict with existing laws.

- Recently the privacy regulation stemming from GLBA was amended to eliminate the annual notice if the agency did not “share” other than within the stated exceptions and if there was no change in agency practices). This improvement, based on needless costs without tangible benefit to the consumer, would no longer be available in this new model.
- No language accounts for the size and complexity of the licensee, a factor that is considered in many other laws and regulations. Understanding and complying with this complex patchwork of requirements, with considerable overlap, would be a costly endeavor for the majority of our members.
- Definitions should be clear that an entity is either a licensee or a third-party service provider but not both to avoid duplicative and possibly incompatible requirements.
- As mentioned above, the fact that licensees include both insurers and producers creates obligations that should only apply to one or the other. This imposes restrictions on certain producers which negate some of their rights under law. It might be best to separate the obligations and impose them on insurers and producers separately. But it also implies considering the specific rights of *independent* agencies. Because of the overarching conflict with the American Agency System, we often struggled to offer alternate language. We realize that the legal differentiation between producers as an entire category and producers who are independent agents under the American Agency System creates a significant challenge under this model, but it is essential to recognize.
- Some of the wording is broad enough that it is difficult to fully assess the interactions with normal agency operations that are necessary both to service the consumer and to protect all parties from potential litigation or future disputes (such as access to, modification of and requests to delete records).
- A section-by-section review is attached.

Thank you for your consideration of this initial review. Please do not hesitate to contact me if you have any questions.

Sincerely,



Claire Pantaloni, CIC, CISR  
Vice President – Advocacy

Attachment: 1

Cc: Jason Ernest, Esq., President & CEO, IA&B  
John Savant, Government Affairs Director

**Insurance Consumer Privacy Protection Model Law #674**

**2023 Privacy Protections Working Group**

**Contents**

ARTICLE 1. GENERAL PROVISIONS..... 3  
    Section 1. Purpose and Scope.....3  
    Section 2. Oversight of Third-Party Service Provider Arrangements .....4  
    Section 3. Definitions .....5  
ARTICLE II. OBLIGATIONS HANDLING CONSUMER'S PERSONAL INFORMATION..... 16  
    Section 4. Data Minimization and Sharing Limitations ..... 16  
    Section 5. Retention and Deletion of Consumers' Information..... 19  
ARTICLE III. NOTICES AND AUTHORIZATIONS..... 21  
    Section 6. Initial and Annual Notice of Consumer Information Practices.....21  
    Section 7. Content of Consumer Information Practices Notices .....22  
    Section 8. Delivery of Notices Required by This Act.....25  
    Section 9. Consumers' Consent- How Obtained .....26  
    Section 10. Content of Authorizations .....28  
ARTICLE IV. CONSUMERS' RIGHTS ..... 30  
    Section 11. Access to Personal Information.....30  
    Section 12. Correction or Amendment of Personal Information.....31  
    Section 13. Nondiscrimination and Nonretaliation ..... 32  
ARTICLE V. ADVERSE UNDERWRITING DECISIONS; OTHER TRANSACTIONS [OPTIONAL] ... 34  
    Section 14. Adverse Underwriting Decisions .....34  
    Section 15. Information Concerning Previous Adverse Underwriting-Decisions.....35  
    Section 16. Previous Adverse Underwriting-Decisions .....35  
ARTICLE VI. ADDITIONAL PROVISIONS ..... 36  
    Section 17. Pretext Interviews [OPTIONAL] .....36  
    Section 18. Investigative Consumer Reports [OPTIONAL].....36  
    Section 19. Compliance with HIPAA and HITECH .....37  
ARTICLE VII GENERAL PROVISIONS..... 38  
    Section 20. Power of Commissioner .....38  
    Section 21. Confidentiality.....38  
    Section 22. Record Retention .....39  
    Section 23. Hearings, Records, and Service of Process .....39  
    Section 24. Service of Process -Third-Party Service Providers.....40  
    Section 25. Cease and Desist Orders and Reports.....41



**Insurance Consumer Privacy Protection Model Law #674**

**2023 Privacy Protections Working Group**

Section 26. Penalties.....41  
Section 27. Judicial Review of Orders and Reports .....42  
Section 28. Individual Remedies.....43  
Section 29. Immunity.....44  
Section 30. Obtaining Information Under False Pretenses .....44  
Section 31. Severability.....44  
Section 32. Conflict with Other Laws .....44  
Section 33. Rules and Regulations .....44  
Section 34. Effective Date .....45

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

#### ARTICLE 1. GENERAL PROVISIONS

##### Section 1. Purpose and Scope

- A. **Purpose:** This Act establishes (i) standards for the collection, processing, retaining, or sharing of consumers' personal information by licensees to maintain a balance between the need for information by those in the business of insurance and consumers' need for fairness and protection in the use of consumers' personal information; (ii) standards for additional permitted transactions involving consumers' personal information; and (iii) standards applicable to licensees for notice to consumers of the collection, processing, retention, or sharing of consumers' personal information. These standards address the need to:
- (1) Limit the collection, processing, retention, or sharing of consumers' personal information to purposes required in connection with insurance transactions and additional permitted transactions ;
  - (2) Enable consumers to determine what personal information is collected, processed, retained, or shared;
  - (3) Enable consumers to know the sources from whom consumers' personal information is collected and with whom such information is shared;
  - (4) Enable consumers to understand why and for generally how long personal information is retained;
  - (5) Allow individual consumers to access personal information relating to the consumer requesting access, to verify or dispute the accuracy of the information; and
  - (6) Allow consumers to obtain the reasons for adverse underwriting transactions.
- B. **Scope:** The obligations imposed by this Act shall apply to licensees and third-party service providers, on or after the effective date of this Act:
- (1) Collect, process, retain, or share consumers' personal information in connection with insurance transactions;
  - (2) Engage in insurance transactions with consumers; or
  - (3) Engage in additional permitted transactions involving consumers' personal information.
- C. **Protections:** The rights granted by this Act shall extend to consumers:
- (1) Who are the subject of information collected, processed, retained, or shared in connection with insurance transactions;
  - (2) Who engage in or seek to engage in insurance transactions;

Commented [KJ1]: Based on Model 670

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (3) Who have engaged in the past in insurance transactions with any licensee or third-party service provider; or
- (4) Whose personal information is used in additional permitted transactions by licensees and third-party service providers.

**Drafting Note:** This model is intended to include the protections for consumers that are provided by NAIC Model Law #670 and NAIC Model Regulation #672 and adds additional protections that reflect the business practices in the insurance industry today. The business of insurance is more global than it was 30-40 years ago. This model law reflects those realities and addresses the need for additional protections for consumers. This model requires notices to consumers for various privacy concerns and will supplant any notices required under Model #670, Model #672 and Gramm-Leach Bliley.

### Section 2. Oversight of Third-Party Service Provider Arrangements

- A. A licensee shall exercise due diligence in selecting its third-party service providers. No licensee shall (i) engage a third-party service provider to collect, process, or retain, or share any consumer's personal information, or (ii) share any consumer's personal information with any third-party service provider for any purpose unless there is a written agreement between the licensee and third-party service provider that requires the third-party service provider to abide by the provisions of this Act and the licensee's own practices in the collection, processing, retention, or sharing of any consumer's personal information.
- B. A licensee shall require all the licensee's third-party service providers to implement appropriate measures to comply with the provisions of this Act in relation to consumers' personal information that is (i) collected, processed, or retained by or (ii) shared with or otherwise made available to the third-party service providers in connection with (i) any insurance transactions of the licensee or (ii) any additional permitted transactions.
- C. No agreement or contract between a licensee and a third-party service provider shall permit the third-party service provider to collect, process, retain, or share any consumer's personal information in any manner:
  - (1) Not permitted by this Act; and
  - (2) Not consistent with the licensee's own privacy practices.
- D. An agreement between a licensee and third-party service provider shall require that no third-party service provider shall further share or process a consumer's personal information other than as specified in the agreement with the licensee.

Commented [KJ2]: Language taken from Model 668 (IDSA)

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

#### Section 3. Definitions

As used in this Act:

A. "Address of record" means:

- (1) A consumer's last known USPS mailing address shown in the licensee's records; or
- (2) A consumer's last known email address as shown in the licensee's records, if the consumer has consented under [refer to the state's UETA statute] to conduct business electronically.
- (3) An address of record is deemed invalid if
  - (a) USPS mail sent to that address by the licensee has been returned as undeliverable and if subsequent attempts by the licensee to obtain a current valid address for the consumer have been unsuccessful; or
  - (b) The consumer's email address in the licensee's records is returned as "not-deliverable" and subsequent attempts by the licensee to obtain a current valid email address for the consumer have been unsuccessful.

Commented [KJ3]: The language in this subdivision was taken from Model 672.

B. "Additional permitted transactions" means collecting, processing, retaining, or sharing a consumer's personal information, with the consumer's consent, for:

- (1) Marketing purposes; or
- (2) Research activities not related to rating or risk management purposes for or on behalf of the licensee.

C. Adverse underwriting decision means:

- (1) Any of the following actions with respect to insurance transactions involving primarily personal, family, or household use:
  - (a) A denial, in whole or in part, of insurance coverage requested by a consumer;
  - (b) A termination of insurance coverage for reasons other than nonpayment of premium;
  - (c) A rescission of the insurance policy;
  - (d) ~~Failure of a producer to apply for insurance coverage with a specific insurer represented by the producer and that is requested by a consumer.~~
  - (e) In the case of a property or casualty insurance coverage:

Commented [KJ4]: By limiting AUDs in this manner, we provide consistency with current state law (for those states that adopted Model 670 and consistency with FCRA).

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (i) Placement by an insurer or producer of a risk with a residual market mechanism, non-admitted insurer, or an insurer that specializes in substandard risks;
  - (ii) The charging of a higher rate based on information which differs from that which the consumer furnished; or
  - (f) In the case of a life, health, or disability insurance coverage, an offer to insure at higher than standard rates.
- (2) Notwithstanding subsection C 1, the following insurance transactions shall not be considered adverse underwriting decisions but the insurer or producer responsible for the occurrence shall provide the consumer with the specific reason or reasons for the occurrence in writing:
- (a) The termination of an individual policy form on a class or state-wide basis;
  - (b) A denial of insurance coverage solely because such coverage is not available on a class- or state-wide basis; or
  - (c) If requested by a consumer, any other insurer-initiated increase in premium on an insurance product purchased by a consumer.

**Drafting Note:** The use of the term “substandard” in Section 2B(d)(1) is intended to apply to those insurers whose rates and market orientation are directed at risks other than preferred or standard risks. To facilitate compliance with this Act, Commissioners should consider developing a list of insurers operating in their state which specialize in substandard risks and make it known to insurers and producers.

- D. “Affiliate” or “affiliated” means a person that directly, or indirectly through one or more intermediaries, controls, is controlled by, or is under common control with another person.
- E. “Biometric information” means an individual’s physiological, biological, or behavioral characteristics that can be used, singly or in combination with each other or with other identifying information, to establish a consumer’s identity. Biometric information includes deoxyribonucleic acid (DNA), imagery of the iris, retina, fingerprint, face, hand, palm, ear, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.
- F. “Clear and conspicuous notice” means a notice that is reasonably understandable and designed to call attention to the nature and significance of its contents.
- G. “Collect” or “collecting” means buying, renting, gathering, obtaining, receiving, or accessing any consumers’ personal information by any means.

**Commented [KJ5]:** Language from Model 672 in part.

**Commented [KJ6]:** Model 672 definition only applies to identified data: to obtain information that the licensee organizes or can retrieve by the name of an individual or by identifying number, symbol or other identifying particular assigned to the individual, irrespective of the source of the underlying information

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- H. “Commissioner” means [insert the appropriate title and statutory reference for the principal insurance regulatory official of the state].
- I. “Consumer” means an individual and the individual’s legal representative, including a current or former (i) applicant, (ii) policyholder, (iii) insured, (iv) beneficiary, (v) participant, (vi) annuitant, (vii) claimant, or (viii) certificate holder who is a resident of this state and whose personal information is used, may be used, or has been used in connection with an insurance transaction. An individual that is a mortgagor of a mortgage covered under a mortgage insurance policy is a consumer. A consumer shall be considered a resident of this state if the consumer’s last known mailing address, as shown in the records of the licensee, is in this state unless the last known address of record is deemed invalid.
- J. “Consumer report” means a written, oral, or other communication of information bearing on a consumer’s creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used in connection with an insurance transaction.
- K. “Consumer reporting agency” means a person who:
- (1) Regularly engages, in whole or in part, in the practice of assembling or preparing consumer reports for a monetary fee;
  - (2) Obtains information primarily from sources other than insurers; and
  - (3) Furnishes consumer reports to other persons.
- L. “Control” means:
- (1) Ownership, control, or power to vote twenty-five percent (25%) or more of the outstanding shares of any class of voting security of the company, directly or indirectly, or acting through one or more other persons;
  - (2) Control in any manner over the election of a majority of the directors, trustees or general partners (or individuals exercising similar functions) of the company; or
  - (3) The power to exercise, directly or indirectly, a controlling influence over the management or policies of the company, as the commissioner determines.
- M. “Delete” and “deleted” means to remove or destroy information such that it is not maintained in human or machine-readable form and cannot be retrieved or utilized in such form;
- N. “De-identified” means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a licensee that uses de-identified information:

Commented [KJ7]: This definition is similar to that in Model 672.

Commented [KJ8]: Definition from Model 672

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (1) Has implemented technical safeguards designed to prohibit re-identification of the consumer to whom the information may pertain.
  - (2) Has implemented reasonable business policies that specifically prohibit re-identification of the information.
  - (3) Has implemented business processes designed to prevent inadvertent release of de-identified information.
  - (4) Makes no attempt to re-identify the information.
- O. "Health care" means:
- (1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care, services, procedures, tests, or counseling that:
    - (a) Relates to the physical, mental, or behavioral condition of an individual; or
    - (b) Affects the structure or function of the human body or any part of the human body, including the banking of blood, sperm, organs, or any other tissue; or
  - (2) Prescribing, dispensing, or furnishing drugs or biologicals, or medical devices, or health care equipment and supplies to an individual.
- P. "Health care provider" means a health care practitioner licensed, accredited, or certified to perform specified health care consistent with state law, or any health care facility.
- Q. "Health information" means any consumer information or data except age or gender, created by or derived from a health care provider or the consumer that relates to:
- (1) The past, present, or future (i) physical, (ii) mental, or (iii) behavioral health, or condition of an individual;
  - (2) The genetic information of an individual;
  - (3) The provision of health care to an individual; or
  - (4) Payment for the provision of health care to an individual.
- R. "Individual" means a natural person;
- S. "Institutional source" means any person or governmental entity that provides information about a consumer to a licensee other than:
- (1) A producer;
  - (2) A consumer who is the subject of the information; or

Commented [KJ9]: Taken from Model 672

Commented [KJ10]: This definition comes from Model 672

Commented [KJ11]: This definition comes from Model 672

Commented [KJ12]: WG added this update to the definition

Commented [KJ13]: Model 670

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (3) An individual acting in a personal capacity rather than in a business or professional capacity.
- T. "Insurance support organization" means:
- (1) Any person who regularly engages in the collection, processing, retention, or sharing of consumers' information for the primary purpose of providing insurers or producers information in connection with insurance transactions, including:
    - (a) The furnishing of consumer reports or investigative consumer reports to licensees or other insurance support organizations for use in connection with insurance transactions,
    - (b) The collection of personal information from licensees or other insurance support organizations to detect or prevent fraud, material misrepresentation, or material nondisclosure in connection with insurance transactions.
    - (c) The collection of any personal information in connection with an insurance transaction that may have application in transactions in other than an insurance transaction.
  - (2) Notwithstanding Subdivision (1) of this subsection, producers, government institutions, insurers, health care providers shall not be considered "insurance support organizations" for purposes of this Act.
- U. "Insurance transaction" means any transaction or service by or on behalf of a licensee involving:
- (1) The determination of a consumer's eligibility for or the amount of insurance coverage, rate, benefit, payment, or claim settlement;
  - (2) The servicing of an insurance application, policy, contract, or certificate, or any other insurance product;
  - (3) Provision of "value-added services or benefits" in connection with an insurance transaction;
  - (4) Any mathematical-based decision that involves a consumer's personal information; or
  - (5) Any actuarial or research studies for rating or risk management purposes conducted by or for the benefit of the licensee using consumers' personal information.
- V. "Insurer" means
- (1) Any person or entity required to be licensed by the commissioner to assume risk, or otherwise authorized under the laws of the state to assume risk,

Commented [KJ14]: Model 670

Commented [KJ15]: Model 672 uses "Insurance product or service" means any product or service that is offered by a licensee pursuant to the insurance laws of this state.  
(2) Insurance service includes a licensee's evaluation, brokerage or distribution of information that the licensee collects in connection with a request or an application from a consumer for a insurance product or service.



## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

including any corporation, association, partnership, nonprofit hospital, medical or health care service organization, health maintenance organization, reciprocal exchange, inter insurer, Lloyd's insurer, fraternal benefit society, or multiple-employer welfare arrangement;

- (2) A self-funded plan subject to state regulation.
- (3) A preferred provider organization administrator.
- (4) "Insurer" does not include producers, insurance support organizations, foreign-domiciled risk retention groups, or foreign-domiciled reinsurers.

**Drafting Note:** If the state regulates third party administrators who operate on behalf of insurers, the state may wish to add them to this list.

W. "Investigative consumer report" means a consumer report or portion of a consumer report in which information about an individual's character, general reputation, personal characteristics, or mode of living is obtained through personal interviews with the individual's neighbors, friends, associates, acquaintances, or others who may have knowledge concerning such items of information.

Commented [KJ16]: Definition from Model 670

X. "Licensee" means 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. "Licensee" shall also include an unauthorized insurer that accepts business placed through a licensed excess lines broker in this state, but only in regard to the excess lines placements placed pursuant to Section [insert section] of the state's laws.

Commented [KJ17]: This definition was taken from Model 668 but is very similar to the definition in Model 672

Y. "Nonaffiliated third party" means:

Commented [KJ18]: Model 672

- (1) Any person except:
  - (a) An affiliate of a licensee; or
  - (b) A person employed jointly by a licensee and any company that is not an affiliate of the licensee; however, a nonaffiliated third party includes the other company that jointly employs the person.
- (2) Nonaffiliated third party includes any person that is an affiliate solely by virtue of the direct or indirect ownership or control of the person by the licensee or its affiliate in conducting merchant banking or investment banking activities of the type described in Section 4(k)(4)(H) or insurance company investment activities of the type described in Section 4(k)(4)(I) of the federal Bank Holding Company Act (12 U.S.C. 1843(k)(4)(H) and (I)).

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- Z. "Nonpublic Information" means information that is not publicly available information and is:

Commented [KJ19]: From Model 672

Any information concerning a consumer which because of name, number, personal mark, or other identifier can be used to identify such consumer, in combination with any one or more of the following data elements:

- (1) Social Security number,
- (2) Driver's license number or non-driver identification card number,
- (3) Account number, credit or debit card number,
- (4) Any security code, access code or password that would permit access to a consumer's financial account, or
- (5) Biometric information;

- AA. "Person" means any individual, corporation, association, partnership, or other legal entity.

- BB. "Personal information" means:

- (1) Any individually identifiable information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked to a consumer that is:

Commented [KJ20]: From Model 670

- (a) Gathered in connection with an insurance transaction;
- (b) Gathered in connection with any other permitted transaction;

- (2) Any of the following:

- (a) Account balance information and payment history;
- (b) The fact that an individual is or has been one of the licensee's customers or has obtained an insurance product or service from the licensee;
- (c) Any information about the licensee's consumer if it is disclosed in a manner that indicates that the individual is or has been the licensee's consumer, unless such disclosure is required by federal or state law for reporting purposes;
- (d) Any information that a consumer provides to a licensee or that the licensee or its agent otherwise obtains in connection with collecting on a loan or servicing a loan;
- (e) Any information the licensee collects through an information-collecting device from a web server, such as internet cookies;
- (f) Information from a consumer report;

Commented [KJ21]: The information in F(1) (b)-(g) was taken directly from Model 672

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (g) Information that would enable judgments, directly or indirectly, to be made about a consumer's character, habits, avocations, finances, occupation, general reputation, credit, health, or any other personal characteristics; or
- (3) "Nonpublic information";
- (4) "Publicly available information;"
- (5) "Sensitive personal information";
- (6) "Health information;" or
- (7) Consumers' demographic data, in any form or medium that can reasonably be used to identify an individual.
- (8) "Personal information" includes collections or sets of individually identifiable information pertaining to more than one consumer.
- (9) "Personal information" does not include "de-identified information."
- CC. "Pretext interview" means an attempt to obtain information about an individual, where an interviewer does one or more of the following:
- (1) Pretends to be someone the interviewer is not;
- (2) Pretends to represent a person the interviewer is not in fact representing;
- (3) Misrepresents the true purpose of the interview; or
- (4) Refuses to provide identification upon request.
- DD. "Precise geolocation" means any data that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet.
- EE. "Process" or "processing" mean: any operation or set of operations performed by a licensee, whether by manual or automated means, on the personal information of any consumer, including the collection, use, sharing, storage, disclosure, analysis, deletion, retention, or modification of data or personal information.
- FF. "Privileged information" means any personal information that:
- (1) Relates to a claim for insurance benefits or a civil or criminal proceeding involving a consumer; and
- (2) Is collected in connection with or in reasonable anticipation of a claim for insurance benefits or civil or criminal proceeding involving a consumer;

Commented [KJ22]: The provision in F.(1)(h) was taken from Model 670

Commented [KJ23]: Model 670

Commented [KJ24]: Model 670

**Drafting Note:** The phrase "in reasonable anticipation of a claim" contemplates that the insurer has actual knowledge of a loss but has not received formal notice of the claim.

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

GG. "Producer" means [refer here to every appropriate statutory category of producer, including brokers, required to be licensed to do business in the state].

**Drafting Note:** This is necessary because many states have various terms for producers, or for producers of certain types of insurers.]

HH. "Publicly available" means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from:

- (1) Federal, state, or local government records;
- (2) Widely distributed media; or
- (3) Disclosures to the general public that are required to be made by federal, state or local law.

**Commented [KJ25]:** This definition comes from the IDSA (Model 668) and Model 672

**Drafting Note:** Examples of "a reasonable basis" are: (1) A licensee has a reasonable basis to believe that mortgage information is lawfully made available to the general public if the licensee has determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded or (2) A licensee has a reasonable basis to believe that an individual's telephone number is lawfully made available to the general public if the licensee has located the telephone number online or the consumer has informed you that the telephone number is not unlisted.

**Commented [KJ26]:** Examples take from Model 672

II. "Residual market mechanism" means an association, organization or other entity defined or described in Sections(s) [insert those sections of the state insurance code authorizing the establishment of a FAIR Plan, assigned risk plan, reinsurance facility, joint underwriting association, etc.]

**Commented [KJ27]:** Model 670 language

**Drafting Note:** Those states having a reinsurance facility may want to exclude it from this definition if the state's policy is not to disclose to insureds the fact that they have been reinsured in the facility.

JJ. "Retain" "retention" or "retaining" means storing or archiving personal information that is in the continuous possession, use, or control of licensee or a third-party service provider.

KK. "Sensitive personal information" means information that reveals (i) a consumer's social security, driver's license, state identification card, or passport number; (ii) a consumer's account log-in or financial account, debit card, or credit card numbers in combination with any required security or access code, password, or credentials allowing access to an account; (iii) a consumer's precise geolocations; (iv) a consumer's racial or ethnic origin, religious, or philosophical beliefs; (v) union membership; (vi) the contents of a consumer's personal mail, personal email, and personal text messages unless the person in possession is the intended recipient of the communication; (vii) a consumer's genetic data; (viii) a consumer's sex life or sexual orientation; (ix) a consumer's citizenship or immigration status; (x) a consumer's health information; or (xi) a consumer's biometric information.

**Drafting Note:** Those states that have enacted a consumer data protection act may want to amend this definition to match that of the state's law.

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

LL. “Share,” “shared,” or “sharing” means (i) disclosing, (ii) disseminating, (iii) making available, (iv) releasing, (v) renting, (vi) transferring, (vii) selling, or (viii) otherwise communicating by any means, a consumer’s personal information (i) by a licensee to an insurance support organization or (ii) a licensee or insurance support organization to a third-party service provider, whether or not for monetary or other valuable consideration, including other permitted transactions between a licensee and an insurance support organization or a licensee or insurance support organization and a third party service provider for the benefit of any party in which no valuable consideration is exchanged.

MM. “Termination of insurance coverage” or “termination of an insurance policy” means either a cancellation or nonrenewal of an insurance policy, in whole or in part, for any reason other than failing to pay a premium as required by the policy.

NN. “Third-party service provider” means any person that obtains consumers’ personal information from a licensee or provides consumers’ personal information to a licensee or that:

(1) (a) Has access to consumers’ personal information through the person’s provision of: (i) any services to or on behalf of a licensee; (ii) electronic applications for use by the licensee’s consumers; or (iii) any other products to or on behalf of the licensee in connection with insurance transactions; or (iv) the provision of services in connection with additional permitted transactions; and

(b) Is either (i) an insurance support organization; or (ii) any person not otherwise defined as a licensee; or

(2) Is a vendor of personal health records.

OO. “Unauthorized insurer” means an insurer that has not been granted a certificate of authority by the Commissioner to transact the business of insurance in this state.

**Drafting Note:** Each state must make sure this definition is consistent with its surplus lines laws.

PP. “Value-added service or benefit” means a product or service that:

(1) Relates to insurance coverage applied for or purchased by a consumer; and

(2) Is primarily designed to satisfy one or more of the following:

(a) Provide loss mitigation or loss control;

(b) Reduce claim costs or claim settlement costs;

(c) Provide education about liability risks or risk of loss to persons or property;

Commented [KJ28]: Model 670

Commented [KJ29]: From Model 668 but modified for this model

Commented [KJ30]: Definition from Model 670

Commented [KJ31]: This definition was taken primarily from Model 880 (rebating)

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (d) Monitor or assess risk, identify sources of risk, or develop strategies for eliminating or reducing risk;
- (e) Enhance the health of the consumer, including care coordination;
- (f) Enhance financial wellness of the consumer through education or financial planning services;
- (g) Provide post-loss services;
- (h) Incentivize behavioral changes to improve the health or reduce the risk of death or disability of a customer (defined for purposes of this subsection as policyholder, potential policyholder, certificate holder, potential certificate holder, insured, potential insured or applicant); or
- (i) Assist in the administration of employee or retiree benefit insurance coverage.

**Drafting Note:** Examples of “value-added services and benefits” are services or benefits related to (i) health and wellness, (ii) telematic monitoring, or (iii) property replacement services.

QQ. “Written consent” means any method of capturing a consumer’s consent that is capable of being recorded or maintained for as long as the licensee has a business relationship with a consumer; or the licensee or service provider is required to maintain the information as provided in this Act.

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

#### ARTICLE II. OBLIGATIONS HANDLING CONSUMER'S PERSONAL INFORMATION

##### Section 4. Data Minimization and Sharing Limitations

- A. No licensee shall collect, process, retain, or share a consumer's personal information unless:
- (1) The collection, processing, retention, or sharing is in connection with an insurance transaction as defined in this Act;
  - (2) The licensee provides the applicable notices required by this Act;
  - (3) The collection, processing, retention, or sharing of the consumer's personal information is consistent with and complies with the most recent notice provided to the consumer by the licensee;
  - (4) The collection, processing, retention, or sharing of the consumer's personal information is reasonably necessary and proportionate to achieve the purposes related to the requested insurance transaction or additional permitted transactions and not further processed, retained, or shared in a manner that is incompatible with those purposes; and
  - (5) The licensee or third-party service provider has obtained prior consent from any consumer whose personal information will be:
    - (a) Used in connection with an additional permitted transaction, as defined in this Act; or
    - (b) Shared with a person outside the jurisdiction of the United States, or its territories, as provided in this Act.
- B. Consistent with the requirements of this Act, a licensee may collect, process, retain, or share a consumer's personal information in connection with an insurance transaction as necessary:
- (1) For the servicing of any insurance application, policy, contract, or certificate under which the consumer is an actual or prospective insured, claimant, or beneficiary;
  - (2) For compliance with a legal obligation to which the licensee is subject;
  - (3) For compliance with a request or directive from a law enforcement or insurance regulatory authority;
  - (4) For compliance with a warrant, subpoena, discovery request, judicial order, or other administrative, criminal, or civil legal process, or any other legal requirement that is binding upon the licensee collecting, processing, retaining, or sharing the personal information;

**Commented [KJ32]:** Most of these requirements were taken from Model 670 Section 13 with some additional restrictions on sharing and processing.

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (5) For a lienholder, mortgagee, assignee, lessor, or other person shown on the records of an insurer or producer as having a legal or beneficial interest in a policy of insurance, to protect that interest provided that:
  - (a) No health information is shared unless the sharing would otherwise be permitted by this section, and
  - (b) The information shared is limited to that which is reasonably necessary to permit such person to protect its interests in such policy;
- (6) To enable a licensee to detect or prevent criminal activity, fraud, material misrepresentation, or material nondisclosure in connection with an insurance transaction;
- (7) To enable a health care provider to:
  - (a) Verify the consumer's insurance coverage or benefits;
  - (b) Inform a consumer of health information of which the consumer may not be aware; or
  - (c) Conduct an operations or services audit to verify the individuals treated by the health care provider; provided only such information is shared as is reasonably necessary to accomplish the audit;
- (8) To permit a party or a representative of a party to a proposed or consummated sale, transfer, merger or consolidation of all or part of the business of the licensee to review the information necessary for such transaction, provided:
  - (a) Prior to the consummation of the sale, transfer, merger, or consolidation only such information is shared as is reasonably necessary to enable the recipient to make business decisions about the purchase, transfer, merger, or consolidation; and
  - (b) The recipient agrees not to share consumers' personal information until
    - (i) consumer privacy protection notices have been provided to the consumers and (ii) the recipient has complied with the provisions of this Act;
- (9) For an affiliate whose only use of the information is to perform an audit of a licensee provided the affiliate agrees not to process personal information for any other purpose or to share the personal information;
- (10) To permit a group policyholder to report claims experience or conduct an audit of the operations or services of a licensee, provided the information shared is reasonably necessary for the group policyholder to make the report or conduct the audit and is not otherwise shared; or

Commented [KJ33]: More restrictive than Model 670



## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (11) To permit (i) a professional peer review organization to review the service or conduct of a healthcare provider provided the personal information is not otherwise processed or shared or (ii) to permit arbitration entities to conduct an arbitration related to a consumer's claim;
  - (12) To provide information to a consumer regarding the status of an insurance transaction; or
  - (13) To permit a governmental authority to determine the consumer's eligibility for health care benefits for which the governmental authority may be liable.
- C. No licensee shall, unless legally required, collect, process, retain, or share a consumer's personal information with an entity outside of the United States and its territories, unless the licensee has provided the required notice and obtained the consumer's prior express consent to do so, as required by Article III of this Act.
- D. No licensee shall permit any of its officers, employees, or agents to collect, process, retain, or share any consumer's personal information, except as relevant and necessary as part of that person's assigned duties.
- E. No licensee may collect, process, retain, or share a consumer's personal information in connection with any additional permitted transactions without consumers' prior express consent. Once consent has been given, any person may conduct marketing, actuarial studies, and research activities as follows:
- (1) For actuarial studies and research activities:
    - (a) No consumer may be identified in any research study or report;
    - (b) All materials allowing the consumer to be identified are returned to the licensee that initiated the actuarial or research study; and
    - (c) A consumer's personal information is deleted as soon as the information is no longer needed for the specific actuarial or research study.
  - (2) For all additional permitted transactions:
    - (a) The person conducting the marketing, actuarial study, or research activity agrees not to further share any consumer's personal information; and
    - (b) A consumer's sensitive personal information may not be shared or otherwise provided to any person for use in connection with any additional permitted transaction.
- F. A licensee may collect, process, retain, or share consumers' de-identified personal information.
- G. No licensee shall:

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (1) Collect, process, retain, or share personal information in a manner inconsistent with the direction of a consumer pursuant to this act; or
  - (2) Collect, process, retain, or share personal information in a manner requiring the prior express consent or authorization of the consumer without obtaining such prior consent.
- H. Notwithstanding any other provision of law, no licensee may sell or share consumers' personal information for any type of consideration.
- I. This section shall not prohibit the collection, processing, retention, or sharing of consumers' personal information to the extent preempted by subdivisions (b)(1)(H) or (b)(2) of Section 625 of the Fair Credit Reporting Act.

### Section 5. Retention and Deletion of Consumers' Information

- A. Once the initial consumer privacy protections notice has been provided to the consumer as set forth in this Act, a licensee may retain a consumer's personal information as necessary for:
- (1) The servicing of an insurance application, policy, contract, or certificate under which the consumer is an actual or prospective insured, claimant, or beneficiary;
  - (2) Compliance with a legal obligation applicable to any insurance transaction involving consumers' personal information to which the licensee is subject;
  - (3) Compliance with a request or directive from a law enforcement or insurance regulatory authority;
  - (4) Compliance with a warrant, subpoena, discovery request, judicial order, or other administrative, criminal, or civil legal process, or other legal requirement that is binding upon a licensee in connection with consumers' personal information;
  - (5) Protection of a legal or beneficial interest in a policy of insurance, with respect to a lienholder, mortgagee, assignee, lessor, or other person shown on the records of an insurer or producer as having a legal or beneficial interest in the policy;
  - (6) Any record retention requirements under any state or federal law applicable to any insurance transaction involving consumers' personal information;
  - (7) Any statute of limitation periods under any state or federal law applicable to any insurance transaction involving consumers' personal information; or

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (8) Any additional permitted transaction provided the consumer has consented in writing to the use of the consumer's personal information for this purpose, the licensee may retain consumer's personal information for as long as the consumer's consent to an additional permitted transaction has not been revoked pursuant to Section 9 of this Act.
- B. Once the provisions of Subsection A of this section are no longer applicable to any of a consumer's personal information held by a licensee:
- (1) Such licensee shall completely delete all the consumer's personal information within 90 days after the provisions in Subsection A of this section no longer apply.
  - (2) Any third-party service provider in possession of the consumer's personal information shall notify the licensee that the consumer's information has been completely deleted.
  - (3) If the licensee no longer has a relationship with the consumer in connection with any insurance transactions, the licensee shall send a notice to the consumer informing the consumer that:
    - (a) The licensee and any third-party service providers no longer retain any of the consumer's personal information and
    - (b) The annual Notice of Consumer Privacy Protections required by Article III of this Act will no longer be sent to the consumer.
  - (4) A licensee shall develop policies and procedures for compliance with this section and be able to demonstrate compliance with those policies and procedures.

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

#### ARTICLE III. NOTICES AND AUTHORIZATIONS

##### Section 6. Initial and Annual Notice of Consumer Information Practices

- A. A licensee that collects, processes, retains, or shares a consumer's personal information in connection with insurance transactions, by whatever means used, shall provide to consumers clear and conspicuous notices that accurately reflect its information policies and practices.
- B. An initial consumer information practices notice shall be provided to a consumer before the licensee, directly or through a third-party service provider, first does any of the following:
- (1) Collects, processes, retains, or shares the consumer's personal information in connection with an application for insurance coverage;
  - (2) Collects, processes, retains, or shares the consumer's personal information in connection with a claim under an insurance policy;
  - (3) Collects the consumer's personal information from a source other than the consumer or public records;
  - (4) Collects, processes, retains, or shares the consumer's personal information in connection with value-added services;
  - (5) Collects, processes, or shares the consumer's personal information in connection with an additional permitted transaction; or
  - (6) Collects, processes, or shares the consumer's personal information, including but not limited to reviewing the consumer's policy or coverage for renewal or reinstatement, if the consumer relationship predates the applicability of this section and the consumer has not already received a ~~notice~~ substantially similar notice.
- C. A further information practice notice shall be provided not less than annually to each consumer with whom the licensee has an ongoing business relationship. The licensee shall conspicuously identify any material changes in its information practices.
- D. The licensee shall honor all representations made to consumers in its most current initial and annual notices, unless otherwise compelled by law, in which case the licensee shall promptly send a notice to all affected consumers explaining the changes in the licensee's information practices. If the licensee's information practices change, the licensee remains bound by the terms of the most recent notice it has given a consumer, until a revised notice has been given.
- E. When a licensee is required to provide a consumer a consent form required by this Act, the licensee shall deliver it according to Section 8.

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

#### Section 7. Content of Consumer Information Practices Notices

- A. The content of any notice required by Section 6 shall state in writing all of the following:
- (1) Whether personal information has been or may be collected from any sources other than the consumer or consumers proposed for coverage, and whether such information is collected by the licensee or by a third-party service provider;
  - (2) The specific types of personal information of the consumer that the licensee or any of its third-party service providers has or may collect, process, retain, or share;
  - (3) The specific purposes for which the licensee collects, processes, retains, or shares personal information as permitted by this Act;
  - (4) The sources that have been used or may be used by the licensee to collect, process, retain, or share the consumer's personal information;
  - (5) That consumers' personal information may be shared for any of the purposes listed permitted in this Act, or a description of the licensee's information practices if those practices are more limited than permitted by this Act;
  - (6) That the consumer may, upon request, obtain a list of any persons with which the licensee or any of the licensee's third-party service providers has shared the consumer's personal information within the current calendar year and, at a minimum, the three previous calendar years.
  - (7) A description of the following requirements as established under Section 4 of this Act:
    - (a) The requirement that the licensee or third-party service provider obtain the consumer's express written consent prior to sharing the consumer's personal information with any person in connection with the collection, processing, retention, or sharing of the consumer's personal information with a person in a jurisdiction outside of the United States and its territories; and the consumer's right to prohibit sharing of the consumer's personal information with such a person;
    - (b) The requirement that the licensee obtain the consumer's express written consent for the collection, processing, retention, or sharing of a consumer's personal information for actuarial purposes unless such information has been de-identified;

Commented [KJ34]: This is language is consistent with Model 910 (Record Retention)

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (c) The requirement that the licensee obtain the consumer's express written consent for the collection, processing, retention, or sharing of a consumer's personal information for research purposes unless such information has been de-identified; and
  - (d) The requirement for the licensee to obtain the consumer's express written consent for the collection, processing, retention, or sharing of a consumer's personal information for marketing a product or service to the consumer;
- (8) A description of the rights of the consumer to access, correct or amend personal information about the consumer and to correct or amend factually incorrect personal information as established under Article IV of this Act, and the instructions for exercising such rights ;
  - (9) A statement of the rights of non-retaliation established under Section 13 of this Act;
  - (10) A summary of the reasons the licensee or any third-party service provider retains personal information and the approximate period of retention; and
  - (11) A statement that no licensee or third-party service provider may sell or share for valuable consideration a consumer's personal information.
  - (12) In addition to the notice provided to consumers, a licensee shall prominently post and make available the notice required by this section on its website, if a website is maintained by the licensee. The licensee shall design its website notice as follows:
    - (a) The notice is clear and conspicuous;
    - (b) The licensee uses text or visual cues to encourage scrolling down the page, if necessary, to view the entire notice and ensure that other elements on the web site (such as text, graphics, hyperlinks, or sound) do not distract attention from the notice, and
    - (c) The licensee either:
      - (i) Places the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or
      - (ii) Places a link on a screen that consumers frequently access, such as a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature, and relevance of the notice.

Commented [KJ35]: This language is from Model 672

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- B. If the licensee uses a consumer's personal information to engage in additional permitted transactions, in addition to the provisions in Subsection A of this section, the following information shall be included in the notice:
- (1) A statement that the consumer may, but is not required to, consent to the collection, processing, sharing, and retention of the consumer's personal information for any additional permitted transactions in which the licensee engages;
  - (2) A description of the reasonable means by which the consumer may express written consent;
  - (3) That the consumer may consent to any one or more of the additional permitted transactions or refuse to consent to any one or more of the additional permitted transactions;
  - (4) That once consent has been given for an additional permitted transaction, the consumer may revoke consent at any time;
  - (5) That once consent for using a consumer's personal information for an additional permitted transaction is withdrawn, the licensee will no longer engage in such additional permitted transaction using the consumer's personal information; and
  - (6) That once consent to an additional permitted transaction has been revoked, any of the consumer's personal information in the possession of the licensee used solely for that additional permitted transaction will be destroyed and deleted as set forth in Section 5 of this Act.
- C. If the licensee shares consumers' personal information with a person who will collect, process, retain, or share consumers' personal information in a jurisdiction outside of the United States and its territories, the following information shall additionally be included in any notice required by Section 6 of this Act:
- (1) A statement that the consumer may, but is not required to, consent to the collection, processing, retention, or sharing, of the consumer's personal information a jurisdiction outside of the United States and its territories;
  - (2) A description of the reasonable means by which the consumer may express written consent;
  - (3) That once consent has been given for the collection, processing, retention, or sharing of consumers' personal information in a jurisdiction outside the United States and its territories, a consumer may revoke consent at any time; and
  - (4) That once consent for the collection, processing, retention, or sharing of consumers' personal information by a person in a jurisdiction outside the United States and its territories has been revoked, any of the consumer's

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

personal information in the possession of such person shall be deleted as set forth in Section 5 of this Act.

- E. The obligations imposed by this section upon a licensee may be satisfied by another licensee or third-party service provider authorized to act on its behalf.

#### Section 8. Delivery of Notices Required by This Act

- A. A licensee shall provide any notices required by this Act so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, electronically pursuant to [state's UETA law].
- B. A licensee may reasonably expect that a consumer will receive actual notice if the licensee:
- (1) Hand-delivers a printed copy of the notice to the consumer;
  - (2) Mails a printed copy of the notice to the address of record of the consumer separately, or in a policy, billing, or other written communication;
  - (3) For a consumer who has agreed to conduct transactions electronically, posts the notice on the electronic site and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular insurance product or service or emails the notice to the consumer and requests a delivery receipt;
- C. A licensee may not, however, reasonably expect that a consumer will receive actual notice of its privacy policies and practices if it:
- (1) Only posts a sign in its office or generally publishes advertisements of its privacy policies and practices; or
  - (2) Sends the notice electronically to a consumer who has not agreed to conduct business electronically with the licensee in connection with an insurance transaction or an additional permitted transaction.
  - (3) Sends the notice electronically to a consumer who has agreed to conduct business electronically with the licensee in connection with an insurance transaction or an additional permitted transaction, but the licensee does not obtain a delivery receipt.
- D. A licensee may reasonably expect that a consumer will receive actual notice of the licensee's annual privacy notice if:
- (1) The consumer uses the licensee's web site to access insurance products and services electronically and agrees to receive notices at the web site and the licensee posts its current privacy notice continuously in a clear and conspicuous manner on the web site; or

Commented [KJ36]: This language comes from Model 672



## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (2) The licensee mails or emails the notice to the consumer's address of record.
  - (3) A licensee may not provide any notice required by this Act solely by orally explaining the notice, either in person or over the telephone.
  - (4) The licensee provides all notices required by this Act so that the consumer can retain them or obtain them later in writing or, if the consumer agrees, electronically.
- E. A licensee may provide a joint notice from the licensee and one or more of its affiliates if the notice accurately reflects the licensee's and the affiliate's privacy practices with respect to the consumer.
- F. If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may satisfy the initial and annual notice requirements of Sections 6 and 7 of this Act, respectively, by providing one notice to those consumers jointly. **The notice must reflect the consent of each consumer.**
- G. If any consumer has requested that the licensee refrain from sending an annual notice of consumer privacy protections and the licensee's current privacy protections notice remains available to the consumer upon request, the licensee shall honor the consumer's request but must continue to send any jointly insured consumer the annual notice.

### Section 9. Consumers' Consent- How Obtained

- A. Where the consumer's consent for the collection, processing, or **sharing** of consumers' personal information by a licensee is required by this Act, a licensee shall provide a reasonable means to obtain written consent and maintain a written record of such consent.
- (2) **A licensee may provide the consent form together with or on the same written or electronic form as the most recent of the initial or annual notice** the licensee provides in accordance with Section 6.
  - (3) If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may provide a single consent notice. Each of the joint consumers may consent or refuse to consent.
  - (4) A licensee does not provide a reasonable means of obtaining express written consent if consent is required or the consumer is instructed that consent is required.
  - (5) A licensee shall comply with a consumer's consent directive as soon as reasonably practicable after the licensee receives it.

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (7) Any consumer who has given consent for the use of personal information in connection with additional permitted transactions, may revoke consent for collection, processing, retention, or sharing of such consumer's personal information. A consumer may exercise the right to consent or to withdraw consent at any time.
  - (8) (a) A consumer's consent directive under this section is effective until the consumer revokes it in writing.  
  
(b) If the consumer subsequently establishes a new relationship with the licensee, the consent directive for any specific activity that applied to the former relationship does not apply to the new relationship. A new relationship occurs when the consumer who previously ended all business relationships with the licensee re-establishes a business relationship more than thirty (30) days after the previous business relationship ended.
  - (9) If the consumer has made conflicting directives pursuant to this section, the consumer's most recent directive for the specific activity shall take precedence.
  - (10) Contracts between a licensee and any third-party service providers shall require either entity receiving to honor the consumer's directive pursuant to this section, and to refrain from collecting, processing, retaining, or sharing the consumer's personal information in a manner inconsistent with the directive of the consumer.
- B. When requesting a consumer's consent to use the consumer's personal information for actuarial studies conducted by a person other than the licensee, or research or marketing activities by anyone, as required by this Act, the consent request shall:
- (1) Be clear and conspicuous;
  - (2) Explain, in plain language, that consent is being sought to use the consumer's personal information for actuarial studies by a person other than the licensee, or for research or marketing activities;
  - (3) Permit the consumer to separately provide consent for use of the consumer's personal information other than sensitive personal information for any one or more additional permitted transactions;
  - (4) Explain, in plain language, that the consumer is not required to provide consent to use the consumer's personal information for any one or all these purposes, and that the consumer will not be subject to retaliation or discrimination as outlined in Section 13, based on the consumer's choice; and
  - (5) State that use of a consumer's sensitive personal information for marketing purposes is prohibited.

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (6) The provisions of Subsection B of this section do not apply to consumers' personal or privileged information that has been de-identified in accordance with this Act.

#### Section 10. Content of Authorizations

Commented [KJ37]: Language from Model 670

- A. No person shall use an authorization for the collection, processing, or sharing of a consumer's personal or privileged information in connection with an insurance transaction unless the authorization meets following requirements.
  - (1) Is written in plain language;
  - (2) Is dated and contains an expiration date for the consent;
  - (3) Specifies the persons authorized to collect, process, or share the consumer's personal or privileged information consistent with the provisions of this Act;
  - (4) Specifies the specific and explicit purposes for which the consumer's personal or privileged information is authorized to be collected, processed, or shared as permitted in Article II of this Act;
  - (5) Names the licensee whom the consumer is authorizing to collect, process, or share the consumer's personal or privileged information;
  - (6) Advises the consumer that they are entitled to receive a copy of the authorization.
- B. No authorization signed by a consumer shall be valid for longer than:
  - (1) For an authorization signed for the purpose of collecting, processing, or sharing a consumer's personal or privileged information in connection with an application for insurance, a reinstatement of an insurance policy, or a request for change in insurance benefits:
    - (a) Twenty-four (24) months from the date the authorization is signed if the application or request involves life, health, or disability insurance; or
    - (b) Ninety (90) days from the date the authorization is signed if the application or request involves property or casualty insurance;
  - (2) For an authorization signed for the purpose of collecting, processing, or sharing a consumer's personal or privileged information in connection with a claim for benefits under an insurance policy, for the duration of the claim.

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (3) For an authorization signed for the purpose of collecting, processing, or sharing a consumer's personal information in connection with loss prevention under an insurance policy, for the duration of the product or service.
- (4) For an authorization signed for the purpose of collecting, processing, or sharing a consumer's personal information in connection with an additional permitted transaction, no longer than 12 months.

**Drafting Note:** The standard established by this section for disclosure authorization forms is intended to supersede any existing requirements a state may have adopted even if such requirements are more specific or applicable to particular authorizations such as medical information authorizations. This section is intended to be the exclusive statutory standard for all authorization forms utilized by licensees. This section does not preclude the inclusion of a disclosure authorization in an application form nor invalidate any disclosure authorizations in effect prior to the effective date of this Act. Nor does this section preclude a licensee from obtaining, in addition to its own authorization form which complies with this section, an additional authorization form required by the person from whom disclosure is sought.

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

#### ARTICLE IV. CONSUMERS' RIGHTS

##### Section 11. Access to Personal Information

- A. Any consumer, after proper identification, may submit a written request to a licensee for access to the consumer's personal information in the possession of the licensee.
- B. The licensee or any third-party service provider shall
  - (1) Acknowledge the request within five (5) business days; and
  - (2) Within fifteen (15) business days from the date such request is received:
    - (a) Disclose to the consumer the identity of those persons to whom the licensee or any third-party service provider has shared the consumer's personal information within the current year and, at a minimum, the three calendar years prior to the date the consumer's request is received.
    - (b) Provide the consumer with a summary of the consumer's personal information and the process for the consumer to request a copy of such information in the possession of the licensee.
    - (c) Identify the source of any consumer's personal information provided to the consumer pursuant to this subsection.
- C. Personal health information in the possession of licensee and requested under Subsection A of this section, together with the identity of the source of such information, shall be supplied either directly to the consumer or as designated by the consumer, to a health care provider who is licensed to provide medical care with respect to the condition to which the information relates. If the consumer elects for the licensee to disclose the information to a health care provider designated by the consumer, the licensee shall notify the consumer, at the time of the disclosure, that it has provided the information to the designated health care provider.
- D. The obligations imposed by this section upon a licensee may be satisfied by another licensee authorized to act on its behalf.
- E. The rights granted to consumers in this section shall extend to any individual to the extent personal information about the individual is collected, processed, retained, or shared by a licensee or its third-party service provider in connection with an insurance transaction or an additional permitted transaction.
- F. For purposes of this section, the term "third-party service provider" does not include "consumer reporting agency" except to the extent this section imposes more stringent requirements on a consumer reporting agency than other state or federal laws.
- G. The rights granted to any consumer by this subsection shall not extend to information about the consumer that is collected, processed, retained, or shared in

Commented [KJ38]: From Model 910

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

connection with, or in reasonable anticipation of, a claim or civil or criminal proceeding involving the consumer.

#### Section 12. Correction or Amendment of Personal Information

- A. Any consumer, after proper identification, may submit a written request to a licensee to correct or amend any personal information about the consumer within the possession of the licensee.
- B. The licensee or any third-party service provider shall
- (1) Acknowledge the request within five (5) business days; and
  - (2) Within fifteen (15) business days from the date such request is received:
    - (a) Correct or amend the personal information in dispute; or
    - (b) If there is a specific legal basis for not correcting or amending the personal information in question, the licensee or its third-party service provider may refuse to make such correction or amendment. However, the licensee refusing to take such action shall provide the following information to the consumer:
      - (i) Written notice of the refusal to make such correction or amendment;
      - (ii) **The basis for the refusal to correct** or amend the information;
      - (iii) The contact information for filing a complaint with the consumer's state insurance regulator, and
      - (iv) The consumer's right to file a written statement as provided in Subsection C of this section.
  - (3) No licensee may refuse to correct or amend a consumer's personal information without good cause, such cause shall be demonstrated to commissioner of the consumer's state insurance department, upon request.
- C. If the licensee corrects or amends personal information in accordance with Subsection A. (1) of this section, the licensee shall so notify the consumer in writing and furnish the correction or amendment to:
- (1) Any person specifically designated by the consumer who may have, received such personal information within the preceding two (2) years;
  - (2) Any insurance support organization whose primary source of personal information is insurers if the insurance support organization has systematically received such personal information from the insurer within the preceding five (5) years; provided, however, that the correction or amendment need not be

Commented [KJ39]: This section is from Model 670 with a shortening of the length of time for B 2

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

furnished if the insurance support organization no longer maintains personal information about the consumer;

- (3) Any third-party service provider that furnished such personal information.
- D. Whenever a consumer disagrees with the refusal of a licensee to correct or amend personal information, the consumer shall be permitted to file with the licensee a concise statement setting forth:
- (1) The relevant and factual information that demonstrates the errors in the information held by the licensee; and
  - (2) The reasons why the consumer disagrees with the refusal of the licensee to correct or amend the personal information.
- E. In the event a consumer files such statement described in Subsection C, the insurer, producer, or insurance support organizations shall:
- (1) Include the statement with the disputed personal information and provide a copy of the consumer's statement to anyone reviewing the disputed personal information; and
  - (2) In any subsequent disclosure by the insurer, producer, or support organization of the personal information that is the subject of disagreement, clearly identify the matter or matters in dispute and include the consumer's statement with the personal information being disclosed.
- F. The rights granted to a consumer by this subsection shall not extend to personal information about the consumer that is collected, processed, retained, or shared in connection with or in reasonable anticipation of a claim or civil or criminal proceeding involving the consumer.
- G. For purposes of this section, the term "insurance support organization" does not include "consumer reporting agency" except to the extent that this section imposes more stringent requirements on a consumer reporting agency than other state or federal law.

### Section 13. Nondiscrimination and Nonretaliation

- A. A licensee and third-party service providers shall not retaliate against a consumer because the consumer exercised any of the rights under this Act.—There shall be a rebuttable presumption that a licensee or third-party service provider has discriminated or retaliated against a consumer if:
- (1) The consumer is required to consent to an additional permitted transaction to obtain a particular product, coverage, rate, or service;

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (2) The consumer is required to consent to an additional permitted transaction in order to provide consent that is otherwise required to obtain an insurance transaction;
- (3) The consumer is required to consent to collection, processing, retention, or sharing of the consumer's information in a jurisdiction outside of the United States and its territories to obtain a particular product, coverage, rate, or service; or
- (4) The consumer is required to consent to collection, processing, retention, or sharing of the consumer's information in a jurisdiction outside of the United States and its territories in order to provide consent that is otherwise required to obtain an insurance transaction.

**Drafting Note:** This section is meant to incorporate similar provisions from Model 672 in this model.

- B. There shall be a rebuttable presumption that consistent with the licensee's filed rules, rates, and forms, and normal underwriting guidelines in the state in which the consumer resides, the following acts do not constitute discrimination or retaliation if the act is reasonably related to any change in price or quality of services or goods applicable to all customers if the licensee is an insurer or a producer, or if a third-party service provider:
- (1) Charges a different rate or premium to the consumer;
  - (2) Provides a different insurance product,
  - (3) Refuses to write insurance coverage for the consumer; or
  - (4) Denies a claim under an insurance product purchased by the consumer.



## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

#### ARTICLE V. ADVERSE UNDERWRITING DECISIONS; OTHER TRANSACTIONS [OPTIONAL]

##### Section 14. Adverse Underwriting Decisions

- A. Notice of an adverse underwriting decision. In the event of an adverse underwriting decision the licensee responsible for the decision shall:
- (1) Either provide in writing to the consumer at the consumer's address of record:
    - (a) The specific reason or reasons for the adverse underwriting decision, or
    - (b) That upon written request the consumer may receive the specific reason or reasons for the adverse underwriting decision in writing; and
  - (2) Provide the consumer with a summary of the rights established under Subsection C of this Section and Sections 11 and 12 of this Act.

**Drafting Note:** Adverse underwriting decisions include: (i) an increase in the risk; (ii) increase in rates in geographical area; (iii) increase base rates; (iv) change in insurance credit score that causes an increase in the premium; (v) the consumer has lost a discount; (vi) an insured had a claim; (vii) a lapse in coverage.

- B. Upon receipt of a written request within ninety (90) business days from the date of a notice of an adverse underwriting decision was sent to a consumer's address of record, the licensee within ten (10) business days from the date of receipt of such request shall furnish to the consumer the following information in writing to the consumer's address of record:
- (1) The specific reason or reasons for the adverse insurance decision, if such information was not initially furnished pursuant to Subsection A(1);
  - (2) The specific information that supports those reasons, provided:
    - (a) A licensee shall not be required to furnish specific privileged information if it has a reasonable suspicion, based upon specific information available for review by the Commissioner, that the consumer has engaged in criminal activity, fraud, material misrepresentation or material nondisclosure, or
    - (b) Health information supplied by a health care provider shall be disclosed either directly to the consumer about whom the information relates or to a health care provider designated by the individual consumer and licensed to provide health care with respect to the condition to which the information relates,
  - (3) A summary of the rights established under Subsection C and Sections 11 and 12 of this Act; and

**Drafting Note:** The exception in Section 10B(2)(a) to the obligation of an insurance institution or agent to furnish the specific items of personal or privileged information that support the reasons for an adverse underwriting decision extends only to information about criminal activity, fraud, material misrepresentation or material nondisclosure that is privileged information and not to all information.

Commented [KJ40]: The provisions in this section are largely from Model 670 with some amendments

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (4) The names and addresses of the sources that supplied the information outlined in Subsection B(2); provided, however, that the identity of any health care provider shall be disclosed either directly to the consumer or to the health care provider designated by the consumer.
- C. The obligations imposed by this section upon a licensee may be satisfied by another licensee authorized to act on its behalf.

#### Section 15. Information Concerning Previous Adverse Underwriting-Decisions

No licensee may make inquiries in connection with an insurance transaction concerning:

- A. Any previous adverse underwriting-decision received by a consumer; or
- B. Any previous insurance coverage obtained by a consumer through a residual market mechanism;

unless such inquiries also request the reasons for any previous adverse underwriting decision or the reasons why insurance coverage was previously obtained through a residual market mechanism.

#### Section 16. Previous Adverse Underwriting-Decisions

No licensee may base an adverse underwriting decision in whole or in part on any of the following:

- A. A previous adverse underwriting decision or that a consumer previously obtained insurance coverage through a residual market mechanism. However, an insurer or producer may base an adverse underwriting decision on further information obtained from a licensee responsible for a previous adverse underwriting decision;
- B. Personal information received from third-party service providers whose primary source of information is insurers. However, a licensee may base an adverse underwriting decision on further supporting information obtained from a third-party service provider; or
- C. Solely on the loss history of the previous owner of the property to be insured.

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

#### ARTICLE VI. ADDITIONAL PROVISIONS

##### Section 17. **Pretext Interviews** [OPTIONAL]

No licensee shall use or authorize the use of pretext interviews to obtain information in connection with an insurance transaction; provided, however, that a pretext interview may be undertaken to obtain information from an individual or legal entity that does not have a generally or statutorily recognized privileged relationship with the consumer about whom the information relates to investigate a claim where, based upon specific information available for review by the Commissioner, there is a reasonable basis for suspecting criminal activity, fraud, material misrepresentation, or material nondisclosure in connection with the claim.

**Drafting Note:** Some states may desire to eliminate the exception in this section and thereby prohibit pretext interviews in all instances. Other states may desire to broaden the exception so that pretext interviews can be utilized in underwriting and rating situations as well as claim situations. States may either expand or limit the prohibition against pretext interviews suggested in this section to accommodate their individual needs and circumstances. Deviation from the standard developed here should not seriously undermine efforts to achieve uniform rules for insurance consumer privacy protections throughout the various states.

Commented [KJ41]: This language with modifications for clarity came from Model 670

##### Section 18. **Investigative Consumer Reports** [OPTIONAL]

- A. No licensee may prepare or request an investigative consumer report about a consumer in connection with an insurance transaction involving an application for insurance, a policy renewal, a policy reinstatement, or a change in insurance benefits unless the licensee informs the consumer in writing prior to the report being prepared that the consumer:
  - (1) May request to be interviewed in connection with the preparation of the investigative consumer report; and
  - (2) Is entitled to receive a copy of the investigative consumer report.
- B. If a licensee prepares an investigative consumer report, the insurer or producer shall conduct a personal interview of a consumer if requested by that consumer.
- C. If a licensee requests a third-party service provider to prepare an investigative consumer report, the licensee requesting such report shall notify in writing the third-party service provider whether a personal interview has been requested by the consumer. The third-party service provider shall conduct the interview requested.
- D. The licensee shall provide a written copy of the investigative consumer report to the consumer.
- E. Notwithstanding Subsections A through D of this section, any licensee that prepares or requests an investigative consumer report in connection with an insurance claim shall notify the consumer that the consumer may request to be interviewed in connection with the preparation of the investigative consumer report. However,

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

neither the licensee nor the third-party service provider is required to provide a copy of an investigative report prepared in connection with an insurance claim unless compelled to do so by a state or federal court.

#### Section 19. Compliance with HIPAA and HITECH

- A. A licensee that is subject to and compliant with the privacy and notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, HITECH), and collects, processes, retains, and shares all personal information in the same manner as protected health information:
- (1) Shall be deemed to comply with Sections 4-8 of this Act provided:
    - (a) The licensee obtains the consent of the consumer prior to engaging in any additional permitted transactions; as defined in this Act; and
    - (b) The licensee obtains all necessary consent of consumers' whose personal information is shared with a person outside the jurisdiction of the United States or its territories, as provided in this Act; and
  - (2) Must comply with the remaining sections of this Act, as applicable.
- B. The licensee shall submit to the [Commissioner] a written statement certifying that the licensee complies with the requirements of Subsections A of this section.
- C. Subsections A and B of this section apply to such licensee if the [Commissioner] has not issued a determination finding that the applicable federal regulations are materially less stringent than the requirements of this Act and if the licensee has complied with the requirements of this section.

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

#### ARTICLE VII GENERAL PROVISIONS

##### Section 20. Power of Commissioner

- A. The Commissioner shall have power to examine and investigate into the affairs of every licensee doing business in this state to determine whether such licensee has been or is engaged in any conduct in violation of this Act.
- B. The Commissioner shall have the power to examine and investigate the affairs of every insurance support organization acting on behalf of a licensee that either transacts business in this state or transacts business outside this state that affects a person residing in this state to determine whether such insurance support organization has been or is engaged in any conduct in violation of this Act.

Commented [KJ42]: This language comes from Model 670

**Drafting Note:** Section 21 B is optional. The drafters included this language for those states that had already adopted Model 670 and those states that wish to adopt this provision.

##### Section 21. Confidentiality

- A. Any documents, materials or other information in the control or possession of the Insurance Department that are furnished by a licensee, third-party service provider, or an employee or agent thereof acting on behalf of the licensee pursuant to this Act, or that are obtained by the Commissioner in an investigation or examination pursuant to [Code Section] shall be confidential by law and privileged, shall not be subject to [insert reference to state open records, freedom of information, sunshine or other appropriate law], shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action. However, the Commissioner is authorized to use the documents, materials, or other information in the furtherance of any regulatory or legal action brought as a part of the Commissioner's duties.
- B. Neither the Commissioner nor any person who received documents, materials or other information while acting under the authority of the Commissioner shall be permitted or required to testify in any private civil action concerning any confidential documents, materials, or information subject to this Act.
- C. To assist in the performance of the Commissioner's duties under this Act, the Commissioner may:
- (1) Share documents, materials or other information, including the confidential and privileged documents, materials or information subject to this Act, with other state, federal, and international regulatory agencies, with the National Association of Insurance Commissioners, its affiliates or subsidiaries, and with state, federal, and international law enforcement authorities, provided that the recipient agrees in writing to maintain the confidentiality and privileged status of the document, material, or other information;
  - (2) Receive documents, materials, or information, including otherwise confidential and privileged documents, materials, or information, from the National

Commented [KJ43]: This language was taken from Model 668 and modified for the purposes of this model.

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

Association of Insurance Commissioners, its affiliates or subsidiaries and from regulatory and law enforcement officials of other foreign or domestic jurisdictions, and shall maintain as confidential or privileged any document, material or information received with notice or the understanding that it is confidential or privileged under the laws of the jurisdiction that is the source of the document, material or information;

- (3) Share documents, materials, or other information subject to this Act, with a third-party consultant or vendor provided the consultant agrees in writing to maintain the confidentiality and privileged status of the document, material, or other information; and
  - (4) Enter into agreements governing sharing and use of information consistent with this subsection.
- D. No waiver of any applicable privilege or claim of confidentiality in the documents, materials, or information shall occur due to disclosure to the Commissioner under this section or due to sharing as authorized in this section.
- E. Nothing in this Act shall prohibit the Commissioner from releasing final, adjudicated actions that are open to public inspection pursuant to [insert appropriate reference to state law] to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates, or subsidiaries.

### Section 22 Record Retention

- A. Notwithstanding any other provision of law, a licensee shall maintain sufficient evidence in its records of compliance with this Act for the calendar year in which the activities governed by this Act occurred and the three calendar years thereafter.
- B. Additionally, a licensee or third-party service provider shall maintain all records necessary for compliance with the requirements of this Act, including, but not limited to:
- (1) Records related to the consumer's right of access pursuant to Article IV;
  - (2) Copies of authorizations and consent\ executed by any consumer pursuant to this Act, for as long as the consumer is in a continuing business relationship with the licensee; and
  - (3) Representative samples of any notice required to be provided to any consumer pursuant to this Act, for as long as the consumer is in a continuing business relationship with the licensee.

Commented [KJ44]: Language from Model 910

### Section 23. Hearings, Records, and Service of Process

Whenever the Commissioner has reason to believe that a licensee or its third-party service providers have been or are engaged in conduct in this state which violates this Act, [ or if the

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

Commissioner believes that a third-party service provider has been or is engaged in conduct outside this state that affects a person residing in this state and that violates this Act], the Commissioner shall issue and serve upon such a licensee or its third-party service provider a statement of charges and notice of hearing to be held at a time and place fixed in the notice. The date for such hearing shall be not less than [insert number] days after the date of service.

- A. At the time and place fixed for such hearing a licensee or its third-party service provider[, or third-party service provider] charged shall have an opportunity to answer the charges against it and present evidence on its behalf. Upon good cause shown, the Commissioner shall permit any adversely affected person to intervene, appear and be heard at such hearing by counsel or in person.
- B. At any hearing conducted pursuant to this section the Commissioner may administer oaths, examine, and cross-examine witnesses and receive oral and documentary evidence. The Commissioner shall have the power to subpoena witnesses, compel their attendance and require the production of books, papers, records, correspondence and other documents, and data that are relevant to the hearing. A record of the hearing shall be made upon the request of any party or at the discretion of the Commissioner. If no record is made and if judicial review is sought, the Commissioner shall prepare a statement of the evidence for use on the review. Hearings conducted under this section shall be governed by the same rules of evidence and procedure applicable to administrative proceedings conducted under the laws of this state.
- C. Statements of charges, notices, orders, and other processes of the Commissioner under this Act may be served by anyone duly authorized to act on behalf of the Commissioner. Service of process may be completed in the manner provided by law for service of process in civil actions or by registered or certified mail. A copy of the statement of charges, notice, order, or other process shall be provided to the person or persons whose rights under this Act have been allegedly violated. A verified return setting forth the manner of service or return receipt in the case of registered or certified mail, shall be sufficient proof of service.

**Drafting Note:** Consideration should be given to the practice and procedure in each state. The items in [] are optional and dependent on the state's authority.

#### Section 24. Service of Process -Third-Party Service Providers

For purposes of this Act, a third-party service provider transacting business outside this state that affects a person residing in this state shall be deemed to have appointed the Commissioner to accept service of process on its behalf; provided the Commissioner causes a copy of such service to be mailed forthwith by registered or certified mail to the third-party

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

service provider at its last known principal place of business. The return receipt for such mailing shall be sufficient proof that the same was properly mailed by the Commissioner.

#### Section 25. Cease and Desist Orders and Reports

- A. If, after a hearing pursuant to Section 23, the Commissioner determines that licensee or its third-party service provider charged has engaged in conduct or practices in violation of this Act, the Commissioner shall reduce his or her findings to writing and shall issue and cause to be served upon such licensee or its third-party service provider a copy of such findings and an order requiring such licensee or its third-party service provider to cease and desist from the conduct or practices constituting a violation of this Act.
- B. If, after a hearing, the Commissioner determines that the licensee or its third-party service provider charged has not engaged in conduct or practices in violation of this Act, the Commissioner shall prepare a written report which sets forth findings of fact and conclusions of law. Such report shall be served upon the insurer, producer, or insurance support organization charged and upon the person or persons, if any, whose rights under this Act were allegedly violated.
- C. Until the expiration of the time allowed for filing a petition for review or until such petition is filed, whichever occurs first, the Commissioner may modify or set aside any order or report issued under this section. After the expiration of the time allowed for filing a petition for review, if no such petition has been duly filed, the Commissioner may, after notice and opportunity for hearing, alter, modify, or set aside, in whole or in part, any order or report issued under this section whenever conditions of fact or law warrant such action or if the public interest so requires.

**Drafting Note:** Consideration should be given to the practice and procedure in each state.

#### Section 26. Penalties

- A. In any case where a hearing pursuant to Section 23 results in the finding of a knowing violation of this Act, the Commissioner may, in addition to the issuance of a cease and desist order as prescribed in Section 25, order payment of a monetary penalty of not more than [dollar amount] for each violation but not to exceed [dollar] in the aggregate for multiple violations.
- B. Any person who violates a cease and desist order of the Commissioner may, after notice and hearing and upon order of the Commissioner, be subject to one or more of the following penalties, at the discretion of the Commissioner:
  - (1) A monetary penalty of not more than [dollar amount] for each violation;



## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (2) A monetary penalty of not more than [dollar amount] if the Commissioner finds that violations have occurred with such frequency as to constitute a general business practice; or
- (3) Suspension or revocation of the license of a licensee.

**Drafting Note:** Consideration should be given to the practice and procedure requirements and penalty requirements in each state.

### Section 27. Judicial Review of Orders and Reports

- A. Any person subject to an order of the Commissioner under [Code cite] or any person whose rights under this Act were allegedly violated may obtain a review of any order or report of the Commissioner by filing in the [insert title] Court of [insert county] County, within [insert number] days from the date of the service of such order or report, a written petition requesting that the order or report of the Commissioner be set aside. A copy of such petition shall be simultaneously served upon the Commissioner, who shall certify and file in such court the entire record of the proceeding giving rise to the order or report which is the subject of the petition. Upon filing of the petition and record the [insert title] Court shall have jurisdiction to make and enter a decree modifying, affirming, or reversing any order or report of the Commissioner, in whole or in part. The findings of the Commissioner as to the facts supporting any order or report, if supported by clear and convincing evidence, shall be conclusive.
- B. To the extent an order or report of the Commissioner is affirmed, the Court shall issue its own order commanding obedience to the terms of the order or report of the Commissioner. If any party affected by an order or report of the Commissioner shall apply to the court for leave to produce additional evidence and shall show to the satisfaction of the court that such additional evidence is material and that there are reasonable grounds for the failure to produce such evidence in prior proceedings, the court may order such additional evidence to be taken before the Commissioner in such manner and upon such terms and conditions as the court may deem proper. The Commissioner may modify his or her findings of fact or make new findings by reason of the additional evidence so taken and shall file such modified or new findings along with any recommendation, if any, for the modification or revocation of a previous order or report. If supported by clear and convincing evidence, the modified or new findings shall be conclusive as to the matters contained therein.
- C. An order or report issued by the Commissioner shall become final:
  - (1) Upon the expiration of the time allowed for the filing of a petition for review, if no such petition has been duly filed; except that the Commissioner may modify or set aside an order or report; or

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (2) Upon a final decision of the [insert title] Court if the court directs that the order or report of the Commissioner be affirmed or the petition for review dismissed.
- D. No order or report of the Commissioner under this Act or order of a court to enforce the same shall in any way relieve or absolve any person affected by such order or report from any liability under any law of this state.

**Drafting Note:** Consideration should be given to the practice and procedure in each state.

### Section 28. Individual Remedies

- A. No Private Cause of Action [OPTIONAL].

Nothing in this Act shall be construed to create or imply a private cause of action for violation of its provisions, nor shall it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.

- B. Private Cause of Action [OPTIONAL]

- (1) If a licensee or one or more of its third-party service providers fail to comply with this Act with respect to the rights granted under this Act, any person whose rights are violated may apply to the [insert title] Court of this state, or any other court of competent jurisdiction, for appropriate equitable relief.
- (2) If a licensee or one or more of its third-party service provider discloses information in violation of this Act, the licensee shall be liable for damages sustained by the individual about whom the information relates; provided, however, that no individual shall be entitled to a monetary award which exceeds the actual damages sustained by the individual.
- (3) In any action brought pursuant to this section, the court may award the cost of the action and reasonable attorney's fees to the prevailing party.
- (4) An action under this section shall be brought within [two (2)] years from the date the alleged violation is or should have been discovered.
- (5) Except as specifically provided in this section, there shall be no remedy or recovery available to individuals, in law or in equity, for occurrences constituting a violation of any provisions of this Act.
- (6) No private cause of action may be brought unless there is an actual victim and actual damages. Damages sought shall be actual damages.
- (7) No claim under this Act may be used to leverage class action litigation.

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

**Drafting Note:** Consideration should be given to the practice and procedure in each state. A state may choose to adopt either Section A or Section B or neither of these sections. However, adopting one or the other of these provisions makes it clearer what the consumers' rights are.

#### Section 29. Immunity

No cause of action in the nature of defamation, invasion of privacy or negligence shall arise against any person for disclosing personal or privileged information in accordance with this Act, nor shall such a cause of action arise against any person for furnishing personal or privileged information to an insurer, producer, or insurance support organization; provided, however, this section shall provide no immunity for disclosing or furnishing false information with malice or willful intent to injure any person.

#### Section 30. Obtaining Information Under False Pretenses

No person shall knowingly and willfully obtain information about a consumer from a licensee under false pretenses. A person found to be in violation of this section shall be fined not more than [insert dollar amount] or imprisoned for not more than [insert length of time], or both.

**Drafting Note:** This provision is applicable to states requiring this language.

#### Section 31. Severability

If any provisions of this Act or the application of the Act to any person or circumstance is for any reason held to be invalid, the remainder of the Act and the application of such provision to other persons or circumstances shall not be affected.

#### Section 32. Conflict with Other Laws

- A. All laws and parts of laws of this state inconsistent with this Act are hereby superseded with respect to matters covered by this Act.
- B. Nothing in this article shall preempt or supersede existing federal or state law related to health information.

#### Section 33. Rules and Regulations

The Commissioner may issue such rules, regulations, and orders as shall be necessary to carry out the provisions of this Act.

**Insurance Consumer Privacy Protection Model Law #674**

**2023 Privacy Protections Working Group**

**Section 34. Effective Date**

This Act shall take effect on [insert a date].



Independent Insurance Agents  
& Brokers of America.

April 3, 2023

Katie Johnson  
Chair  
Privacy Protections Working Group  
National Association of Insurance Commissioners  
1100 Walnut Street, Suite 1500  
Kansas City, MO 64106-2197

*Re: Draft Insurance Consumer Privacy Protections Model Law*

Dear Chair Johnson:

On behalf of the Independent Insurance Agents and Brokers of America (IIABA), the largest insurance agent and broker organization in the country, I write to offer our association's comments and concerns regarding the preliminary draft of the *Insurance Consumer Privacy Protections Model Law*. Our members are the industry constituency that would be most impacted by this proposal, and we appreciate having the opportunity to submit these comments and actively participate in the drafting effort.

### **General Comments**

As we noted in our recent oral testimony to the working group, IIABA and its members are surprised, startled, and troubled by the exposure draft. We recognize this is a very preliminary proposal and one that could change considerably over the weeks and months to come, but it would be impossible to overstate our level of concern at this stage of the process. The draft proposes a radical and unwarranted restructuring of privacy law that would uniquely target one sector of the business world. This proposal would create unnecessary burdens and restrictions for the industry and hinder our ability to serve consumers, and it would have particularly profound and adverse effects on the independent agent system.

Before highlighting some of our most significant substantive concerns with the exposure draft, we wanted to note the following:

- The draft is no doubt the product of the good faith efforts of its drafters, but it extends far beyond the working group's original goals and would establish privacy mandates for the insurance sector that are more onerous and restrictive than the rules applied to other industries. The working group was created to ensure that the NAIC has model laws and recommendations for state policymakers that reflect the marketplace realities of today

and protect consumers in meaningful ways. This is a laudable objective, but the draft proposes a 45-page, top-to-bottom rewriting of privacy law for insurance licensees instead of a more tailored and modest updating of longstanding requirements. Sweeping and disruptive changes in state insurance codes are not needed, and we urge the working group to focus its efforts on addressing any marketplace problems and regulatory gaps that are identified.

- IIABA respectfully encourages the working group to note the privacy measures that are being considered and enacted at the state and federal levels. Although a small number of states have passed comprehensive privacy statutes that may be instructive, it is important to note that the legislatures in these jurisdictions have opted not to apply these frameworks to small businesses or to most insurance licensees. This recent experience suggests there is little interest in a model law that treats the insurance industry in uniquely harsh and unduly restrictive ways or that would impose significant new burdens, costs, and restrictions on main street insurance agents. The goal of the working group is to craft a meaningful and relevant model law that can be uniformly adopted by state legislatures, but broad and unprecedented proposals like the initial draft are unlikely to make their way through the legislative process.
- On a related note, Congress is actively considering revisions to the existing Gramm-Leach-Bliley Act (GLBA) privacy framework, and the House Financial Services Committee recently advanced legislation of this nature. IIABA has urged Congress to ensure that state regulators remain responsible for the implementation and enforcement of the GLBA privacy regime within the insurance industry, but other industry actors are seeking revisions that would largely eliminate the traditional role of the states in this area. The working group's initial draft is viewed as so sweeping and unwarranted that it is being used by some to advance arguments that state officials should lose their regulatory authority under the longstanding GLBA structure.
- The working group noted during its recent open meeting that it has met with more than a dozen insurers and other entities and that it hopes to do so with additional interested parties. IIABA would welcome an opportunity to discuss this proposal, the working group's objectives, and related issues at length. We requested a meeting of this nature two weeks ago and earnestly hope that such a discussion can be arranged in the near future. Our comments below focus on a small number of our most notable concerns and are not exhaustive, but we are happy to chat about privacy and privacy legislation in much greater detail at your convenience. We look forward to your response to our earlier request.
- Responding to this initial draft and attempting to provide meaningful comments has been challenging because it is impossible in some instances to discern why certain provisions were included or drafted in a particular way and what the rationale was for such decisions. Some of the provisions included, for example, would result in some very troubling outcomes, but it is unclear whether these results are intended or inadvertent.<sup>1</sup> If we had a better understanding of the working group's perspective and reasoning, we could perhaps be more responsive and better positioned to provide you with our viewpoints and suggestions.

---

<sup>1</sup> One area of confusion is the manner in which the exposure draft addresses how personal information may be used by licensees, and Sections 4(A), 4(B), and 6(B) all address this topic in slightly different ways.

- As you consider how to address these complex issues, we also urge you look to GLBA Title V as a guide star and to rely on its framework and structure to the extent feasible. Unlike the small number of state comprehensive privacy laws that have been enacted in recent years (which do not even apply to the financial services world), the GLBA privacy regime is crafted with the insurance and other financial sectors in mind. It is the most appropriate and obvious starting point for any insurance industry-specific model law.

## **Specific Comments**

The items discussed below do not represent the entirety of our views concerning the draft, but they do highlight some of our most notable initial concerns.

### Broad and Burdensome Notice Requirements

The draft would dramatically expand privacy notice requirements in numerous and unnecessary ways, and we note several of these below:

- Sections 4 and 6 would require any licensee that receives personal information to provide an information practices notice to a consumer before the information is received. Such a mandate would result in a proliferation of privacy notices in the independent agent context that would confuse and overwhelm consumers. In a scenario in which a consumer engages an independent agent to secure insurance, the consumer would receive a notice from the agent and every company that the agent shares any information with in the process of obtaining quotes (including from those carriers that do not provide a quote or write the business). In a scenario in which an online insurance quote engine is used by a consumer, that person could receive dozens of privacy notices from different insurers. These outcomes provide no consumer benefit and only undermine any value that these disclosures provide.
  - Section 7 addresses the content of information practices notices and would require a level of detail and prescriptiveness that is unduly expansive and incredibly challenging for small licensees. The section is complex and inconsistent with other privacy regimes. The draft would require one to convey the specific types of personal information utilized and name the specific sources of such information, but it would be more appropriate to require disclosure of the “categories” of information and sources. We also urge the working group to examine the information that GLBA Section 503(c) requires to be included in privacy notices and to utilize those thoughtfully crafted and vetted obligations as a starting point for discussion.
- a
- The draft would create an unnecessary duty to deliver information notices annually even when a licensee’s policy is unchanged. This conflicts with the GLBA privacy reforms signed into law by President Obama in 2015 and implemented by insurance and other financial services regulators in the ensuing years. This duplicative and wasteful annual notice obligation should be deleted.
  - Section 5(B) would establish the peculiar requirement that licensees must send notices to consumers to inform them that they will not be receiving any more notices in the future. Paragraphs (2) and (3) of Section 5(B) would establish these unnecessary notice obligations and should simply be deleted.

- The initial notice requirements of Section 6 would require the disclosures to be made *before* a licensee receives information about a consumer, but it would be impossible for licensees to do so in most situations.

### Mandatory Deletion

The working group has stated that it recognizes the need of insurance licensees to retain information for longer than many other types of businesses, yet the draft would require agents to delete personal information unless one of a small number of permissible purposes was met. Specifically, unless one of the narrowly crafted conditions was satisfied, Section 5(B) would require agents and other licensees to “completely delete all of the consumer’s personal information [including information not obtained from the consumer] within 90 days.” Such a framework overlooks the legitimate interests that agents have in maintaining information, harms consumers, and undermines the rights that independent agents have possessed for decades in common law. The draft does not allow data to be maintained for any other legitimate reasons (e.g. to protect against or prepare for claims or other liability), and it would unfairly and inappropriately make it illegal for agents to maintain basic customer files or compete for the business of past clients. This, among other problems, flies in the face of the longstanding rights that agents have to their customer lists and work product and undermines the value of those businesses.

Section 5(A) provides a number of exceptions to the broad deletion mandate, but the list is incomplete. If this deletion obligation is retained in the model, it is imperative that this list be expanded to include additional specific exemptions (e.g. when licensees maintain information to resolve consumer disputes or inquiries, to protect against or prevent claims or other liability, etc.), and the working group should look to GLBA Section 502(e) for guidance. It is impossible, however, for the draft to contemplate every legitimate reason why a licensee might need to retain personal information, so it is critical that the model also permit retention when it is commercially reasonable to do so.

### Prior Consent Obligations

The discussion draft would prohibit insurance agents from using personal information they lawfully possess to engage in marketing or other activities unless they have obtained the consumer’s consent. We do not understand the reasons why the working group would propose to apply such requirements uniquely to the insurance industry, but this framework would be cumbersome, unworkable, and anti-consumer. Agents should not be barred from proactively discussing coverages, helping to fill protection gaps, offering recommendations, and working with insurers to obtain coverages, but this framework would prohibit an agent from marketing other appropriate coverages to a consumer and engaging in other appropriate activities without such consent. We also echo the concerns expressed by others about the manner in which the initial draft would prohibit the sharing of information with an entity outside of the United States without prior consent, and such a mandate would be disruptive for both small agencies and larger institutions. The prior consent framework set forth in the discussion draft must be deleted or significantly revised.

### Universally-Applied Mandates

The working group has indicated that it has looked to recently enacted state consumer data privacy laws for guidance, but it has deviated from the model provided by those statutes in a significant and notable way. Those relatively new privacy laws do not apply to small institutions,



yet the working group's draft would extend all of its new mandates and obligations to even the smallest of licensees. IIABA urges the working group to craft similar exemptions from certain requirements (especially Sections 11 and 12) for insurance producers.

### Third Party Service Providers

The proposal makes agents responsible and strictly liable for the privacy-related activities of service providers with whom they share personal information. This would prohibit an agent from sharing information with an insurer, agency management system vendor, or other provider unless it could compel such entities to enter into specific contractual terms and comply with other demands. Such a system is unrealistic and impractical, and it would not ensure that service providers adhere to such terms and obligations anyway. IIABA strongly opposes these provisions and urges the working group to delete Section 2 and the references to third-party service providers in Section 28.

### Private Cause of Action

For the many reasons discussed during your recent open meeting and in other venues, we strongly urge you to remove the optional private cause of action from the proposal. Creating such a private cause of action is unnecessary and counterproductive, and the effects possibly fall hardest on small and medium-sized enterprises that could be forced to close operations as a result. Enforcement of privacy requirements should remain in the hands of state regulators.

### Purchase/Sale of an Insurance Agency

The inclusion of Section 4(B)(8)(b) would make it practically challenging and perhaps impossible for the buyer of an insurance agency to secure and protect personal information, and we urge the working group to delete this provision. Alternatively, the buyer of an agency should have a reasonable amount of time to provide affected consumers with an information practices notice.

### Prohibition on Sharing Personal Information for Consideration

Section 4(H) would have the practical effect of prohibiting agents from receiving referral fees and sharing commissions when allowed by law, and we urge the working group to delete or redraft this subsection.

### Definitions

A number of definitions will need to be revised, but the definition of "personal information" is an especially critical provision and far too expansive in its current form. Paragraph (1) provides a reasonable starting point, but we urge the working group to delete Paragraph (2) and to expressly exempt "publicly available information" from the definition.

We also wonder why it is necessary to include definitions for "institutional source" and "nonaffiliated third party" as those terms are not used in the body of the initial draft. It is also unclear why the definition of "nonpublic information" is necessary or helpful.

### **Conclusion**

IIABA thanks the working group for its consideration of our views and looks forward to working with you in good faith in the months to come. We welcome the chance to participate in your

open in-person and virtual meetings and also reiterate our request to meet with working group leaders for a more detailed and exhaustive discussion of these issues. If we can provide you with any additional information or assistance in the meantime, please feel free to contact me by phone at 202-302-1607 or via email at [wes.bissett@iiaba.net](mailto:wes.bissett@iiaba.net).

Very truly yours,

A handwritten signature in black ink that reads "Wesley Bissett". The signature is written in a cursive, slightly slanted style.

Wesley Bissett  
Senior Counsel, Government Affairs



*Electronically Submitted to lalexander@naic.org*

April 3, 2023

TO: The NAIC Privacy Protections (H) Working Group (the “Working Group”)

**Re: Exposure Draft of New Consumer Privacy Protections Model Law #674**

Dear Members of the Working Group:

On behalf of our members, the Insured Retirement Institute (IRI)<sup>1</sup> writes to share comments on the Exposure Draft of New Consumer Privacy Protections Model Law #674 (the “Exposure Draft”). We are appreciative of the Working Group’s efforts on this important issue, and we would like to commend the Working Group on its willingness to work with stakeholders throughout the drafting process. We would like to take this opportunity, however, to highlight some of the major concerns for our members. Generally, our members support a principles-based model law that will not be overly prescriptive or restrictive. We believe a draft privacy model should not impede innovation or dramatically alter existing practices, especially since high state adoption will be important to ensure consistency across states. We would also like to note the following specific areas of concern for our members:

- 1) The amount of disclosures/notices required before personal information can even be collected is excessive, and it is unclear if the notices would actually provide value to the consumers. Disclosure can be important, but it must strike a balance between ensuring that the information will be of value to the consumer versus just adding to the overwhelming amount of paper that a consumer receives. Additionally, these disclosures would be added to the current landscape where paper is the default option, and consumers must opt in to receive notices electronically. We question the value of adding more paper notices, especially on top of what is already required under federal and state privacy laws.

---

<sup>1</sup> The Insured Retirement Institute (IRI) is the leading association for the entire supply chain of insured retirement strategies, including life insurers, asset managers, and distributors such as broker-dealers, banks and marketing organizations. IRI members account for more than 95 percent of annuity assets in the U.S., include the top 10 distributors of annuities ranked by assets under management, and are represented by financial professionals serving millions of Americans. IRI champions retirement security for all through leadership in advocacy, awareness, research, and the advancement of digital solutions within a collaborative industry community.

- 2) The burdensome requirements regarding data collected, retained, processed, or shared within jurisdictions outside the United States will have a large operational impact on companies with global operations and will potentially limit the ability of these companies to conduct business.
- 3) Enforcement should be appropriately handled by state regulators, and as such, we recommend that the optional private cause of action provision be removed. The inclusion of such a provision will also likely create inconsistency among states that adopt this model.

We think an appropriate balance needs to be struck between ensuring reasonable privacy protections, consumer expectations regarding modernization, and the need for workable, principles-based requirements. We appreciate the Working Group's consideration of these comments, and please don't hesitate to contact me with any questions or concerns.

Sincerely,

*Sarah E. Wood*

Sarah Wood  
Director, State Policy & Regulatory Affairs  
Insured Retirement Institute  
[swood@irionline.org](mailto:swood@irionline.org)



April 3, 2023

National Association of Insurance Commissioners  
Privacy Protections Working Group  
1100 Walnut Street, Suite 1500  
Kansas City, MO 64106-2197

VIA EMAIL  
[lalexander@naic.org](mailto:lalexander@naic.org)

**Re: Comments to Draft Consumer Privacy Protections Model Law (#674)**

Dear Ms. Alexander:

The International Underwriting Association of London (“IUA”) is pleased to provide the following comments to the draft Consumer Privacy Protections Model Law #674 (“the Draft Model”). The IUA is the representative association for international companies operating in London and providing international wholesale and wholesale insurance and reinsurance coverage. Of the IUA’s 73 ordinary members, most companies write reinsurance in the U.S., and 33 of our members appear on the NAIC’s Quarterly Listing of Alien Insurers to write surplus lines insurance in the U.S.

We welcome the Privacy Protections Working Group’s (“Working Group”) desire to develop a robust model of data privacy protections for insurers operating in the U.S. Nonetheless, the IUA has serious concerns with the proposed application of the Draft Model to non-U.S. excess and surplus lines insurers. Following are our comments for your consideration.

#### **Definition of “Licensee”**

By including unauthorized insurers that accept business through excess lines brokers in its definition of “licensee,” the Draft Model does not take into account existing data privacy practices that such insurers are already subject to, to differing degrees in the UK and U.S. already, and the historical treatment of alien or non-U.S. excess and surplus lines carriers. Moreover, while the Draft Model includes both U.S. and non-U.S. surplus lines insurers in the definition of licensee on the one hand, it simultaneously excludes only “foreign-domiciled reinsurers” from the definition of “insurer.” Many of our members write both U.S. surplus lines insurance and reinsure U.S. cedents. This commercial reality needs to be addressed—in part by excluding both foreign and alien reinsurers, with respect to their U.S. reinsurance business.

In general, a “licensee” in the context of surplus lines business refers to the surplus lines broker, not the insurer, and the surplus lines market is regulated primarily via the broker who is responsible for e.g. diligent search of the admitted market (in some states working with a retail producer), providing disclosure notices to insureds via the retail producer, collecting and paying premium tax, ensuring that the risk in question is appropriate to export to the surplus lines market, etc. Similarly, most existing privacy compliance obligations – such as providing notices to the insured – are fulfilled via the surplus lines broker today. Surplus lines insurers never have direct contact with insureds and must participate in the surplus lines market exclusively via surplus lines brokers. For this reason, the IUA feels that it would be appropriate to amend the definition of licensee so that it includes “brokers that place business with excess or surplus lines insurers” rather than including surplus lines insurers in the definition of licensee directly.

#### **Draft Model vs. GDPR**

The IUA’s members are of course already accustomed to strict privacy regulation in the form of the General Data Protection Regulation (“GDPR”) that has been in place in the United Kingdom and Europe for the past 5 years. That privacy regime in many respects is inconsistent with the Draft Model and risks creating inconsistent compliance obligations. For example, the Draft Model largely proposes a regime which requires consumer

consent/opt-in for many customary business activities such as marketing, while under the GDPR there are well-trodden difficulties with the reliance on consent in the context of a relationship with an imbalance of power, and the difficulties with withdrawal of consent. There are also different marketing requirements under European privacy laws, which include B2B opt-out consent and the possibility of reliance on a “soft” opt-in for direct electronic marketing in certain circumstances.

### **Prior Consent to Transmit Data Outside the U.S. and Data Localization**

The IUA has concerns with the proposal to require prior consent for overseas transactions. There is an obvious practical issue with the prior consent model in relation to alien surplus lines insurers, who are self-evidently not in the U.S. IUA members are alien surplus lines insurers who write surplus lines insurance in the U.S. through a sometimes lengthy broking chain, typically involving at least a retail broker, a surplus lines broker, and a London broker before any customer data reaches the insurer. As such, the insurer is not well-placed to obtain the insured’s consent to send its data overseas, and any applicant for insurance from an alien surplus lines insurer—or the retail producer acting on behalf of the buyer—should already be well-aware that the prospective buyer’s data will be sent overseas when applying for cover. Having to require prior affirmative consent from the applicant would be a cumbersome extra step that would serve only to lengthen the time to apply for insurance from alien surplus lines insurers.

If necessary, rather than prior consent, the IUA suggests that the NAIC could achieve the same goal by requiring the surplus lines broker to disclose at the time of application – either to the applicant if they are dealing with the individual directly, or to the prospective buyer’s retail broker if not – that the applicant’s data may be sent to some non-U.S. surplus lines insurers (in the London Market in particular it is still common for multiple insurers to “subscribe” to underwrite a risk) in order to obtain quotes – in other words, an “opt out” rather than “opt in.” In addition, since the definition of “individual” in the Draft Model includes a “claimant,” it is likely that some third-party claimants in the U.S. with bodily injury or perhaps even property damage claims will have their data sent to alien surplus lines insurers in connection with a claim. Since the insurer requires such data in order to handle the claim, there does not seem to be any purpose to requiring the claimant to consent to sending their data overseas, because the alternative is that the insurer will not be able to determine whether the claim is covered and will not be able to settle the claim.

Further, while we understand the goal of the model to protect consumers’ privacy, any broad requirement to effectively localize data in the U.S. is inconsistent with policy positions and commitments adopted by many developed countries including the U.S. itself, UK, the EU, Japan, Singapore, and Australia. It is inconsistent with positions taken by global regulatory bodies such as the Financial Stability Board and IOSCO. The free flow of data is not, in and of itself, contrary to ensuring data privacy or security.

### **Conflict with the U.S. Regulatory Regime’s Historical Treatment of Excess and Surplus Lines Insurers**

The current proposal appears to be at odds with previous treatment of excess and surplus lines insurers under other NAIC privacy model laws.

The Draft Model is in many respects a merger of two previous models, NAIC Model 670 (originally adopted in 1992) and Model 672 (originally adopted in 2000 post the U.S. passage of the Gramm Leach Bliley Act, which occurred in 1999).

Model 670 did not include surplus lines insurers in its definition of “insurance institutions.” Model 672 through its definition of “licensee” includes unauthorized insurers that accept business through a licensed excess lines broker in a state, but Model 672 applied different obligations to those entities (a prohibition against using such information for non-affiliate marketing and providing a notice), likely in recognition of the differing regulation applied to such excess and surplus carriers historically.

By comparison, the Draft Model applies all of its provisions to excess and surplus lines insurers and subjects them to wide-ranging obligations that belie the historical treatment of such entities when consumer data only

ever reaches them after going through multiple brokers at least some of whom are in the U.S. The provisions of the Draft Model are inconsistent with the most aggressive privacy regimes including in the United States (e.g. the CCPA, which other states have begun to adopt) and abroad (GDPR).

### **Adverse Underwriting Decision**

In the first instance, we do not feel it appropriate for a draft privacy model to include this section as we understand the topic of transparency related to adverse underwriting decisions is being discussed in other NAIC workstreams. However, should the section remain in the model, while we recognize that this language also appeared in Model 670, the IUA believes it is not appropriate to characterize “placement with a non-admitted insurer” as being an adverse underwriting decision. In many cases, the excess and surplus lines market serves as a place to provide new and innovative coverage that is not yet available in the admitted market, and also importantly provides needed capacity in catastrophe-exposed areas, or for high-net worth property owners, professional athletes, and other unusual exposures, none of which should be considered an “adverse underwriting decision” simply because the coverage may not be available in the admitted market. Therefore we would be in favour of removing “placement with a non-admitted insurer” from the definition of “adverse underwriting decision.”

### **Right of Private Action**

Section 28 of the Draft Model provides an option for states adopting the model to either grant a private cause of action to individuals, or to expressly not do so. Given that most recent state privacy legislation in the U.S. does not include similar rights, this is a contentious topic which the IUA does not believe is necessary for the NAIC to address in a model law. The Draft Model already contains extensive provisions for enforcement of the law by insurance commissioners. Whether individuals should have the right to sue is a topic best left to state legislatures, and we recommend that this provision be removed from the Draft Model.

\*\*\*

Thank you for the opportunity to provide comments on the Draft Model. We would be pleased to answer any questions the Working Group may have, or indeed to provide further input in the drafting process.

Yours sincerely



Helen Dalziel  
Director of Public Policy  
**International Underwriting Association**  
T: +44 (0)20 7617 5449  
M: +44 (0)7799 903664  
E: Helen.Dalziel@iua.co.uk



Cc: Thomas M. Dawson—McDermott Will & Emery, LLP  
Andrea Best—McDermott Will & Emery

March 24, 2023

**Via Email**

Ms. Katie Johnson  
Virginia Bureau of Insurance  
Chair, NAIC Privacy Protections (H) Working Group

Re: Exposure Draft of the Insurance Consumer Privacy Protection Model Law (“the Exposure Draft”)

Dear Ms. Johnson:

This comment letter is submitted on behalf of Underwriters at Lloyd's, London (“Lloyd's”) in response to the referenced exposure. Lloyd's is the largest writer of surplus lines insurance in the United States, encompassing business from all 50 states. Surplus lines insurers, which are categorized as unauthorized insurers because they are not required to have a certificate of authority, provide coverage for risks that licensed insurers are either unable or unwilling to write. Because of this ability to fill in coverage gaps, surplus lines insurers are often called the safety-valve of the insurance industry. Lloyd's appreciates the opportunity to provide these comments.

At the onset, we note that Lloyd's is domiciled in the United Kingdom and consequently has been regulated for privacy under the General Data Protection Regulation (“GDPR”) since 2018. As you know, the GDPR is a robust, strict, and well-regarded privacy regime used throughout the European Union and in the UK. Even before the GDPR came into effect, the UK has had a series of increasingly rigorous privacy laws in place since 1984.<sup>1</sup> Lloyd's takes privacy seriously, as does our home jurisdiction.

**Licensee Definition & Transfers Outside the United States**

Lloyd's noted that the Exposure Draft deviates from the typical definition of “licensee” used in most NAIC models by adding a concluding sentence which reads, “Licensee shall also include an unauthorized insurer that accepts business placed through a licensed excess lines broker in this state, but only in regard to the excess lines placements placed pursuant to Section [insert section] of the state's laws.” This sentence is not in the licensee definitions in either Model 688 or 672, nor in Model 670, which collectively serve as the basis for this Exposure Draft. While Lloyd's has no fundamental objection to being regulated for privacy – as stated, the Lloyd's market is already subject to GDPR in the UK – the addition of unauthorized insurers to the licensee definition creates issues throughout the Exposure Draft which need to be considered.

Most notably, the inclusion of unauthorized insurers within the licensee definition makes non-US insurers, i.e. alien insurers, fully subject to the proposed model. However, as presently drafted, the Exposure Draft does not seem to recognize that a significant class of its proposed licensees are based

---

<sup>1</sup> <https://www.ucl.ac.uk/constitution-unit/research/research-archive/foi-archive/what-freedom-information-data-protection#:~:text=The%20development%20of%20Data%20Protection,to%2Ddate%20and%20lawfully%20used.>



outside of the United States. For example, Sections 4(A)(5)(b) and 4(C) prohibit licensees from sharing a consumer's personal information with an entity outside the United States, unless the licensee has provided the required notice and obtained the consumer's prior express consent to do so. These sections do not consider when the licensee is itself based outside the US.

Presumably, the requirement for a licensee to obtain a consumer's prior written consent before sharing personal information outside of the US was added because the drafters thought that sharing information with non-US entities would take that information outside the protections of this model. However, as indicated above, that is not the case because the current Exposure Draft deems non-US entities licensees. Even if the drafters choose to chart a different course and remove the additional language deeming unauthorized insurers licensees, unauthorized insurers would seemingly still be considered third-party service providers to surplus lines brokers, who are themselves licensees, and thus subject to the act's requirements as third-party service providers.

It is illogical to deem non-US entities licensees and/or third-party service providers, yet at the same time require these entities to procure a consumer's prior written consent before sharing data with a person outside the US. The regulation of surplus lines is premised upon the surplus lines broker, as the US licensee, sharing information with the unauthorized carrier, which is frequently based outside the US. Data sharing in this manner is the foundation of the surplus lines industry. In Lloyd's view, there must be a carve out from prohibition against sending data outside the US for alien surplus lines insurers. This holds true even if alien surplus lines insurers are ultimately deemed to be third-party service providers instead of licensees. Surplus lines brokers need to be allowed to transfer consumer personal information about the surplus lines customer to the alien surplus lines insurer. This is a surplus lines broker's statutory duty. Adding the following sentence to Sections 4(A)(5)(b) and 4(C) would accomplish this objective.

*No licensee shall, unless legally required, collect, process, retain, or share a consumer's personal information with an entity outside the United States and its territories, unless the licensee has provided the required notice and obtained the consumer's prior express consent to do so, as required by Article III of this Act. This provision does not apply to the transfer of consumer's personal information to a licensee or third-party service provider which is based outside the United States and is required to comply with the provisions of this Act.*

This change would recognize the established manner in which surplus lines brokers export business to the alien surplus lines market, while still ensuring that a consumer's prior express consent is provided before personal information is shared with any non-US entities not in compliance with the act.

### **Section 3(V) Insurer Definition**

It is worth noting that unauthorized insurers are not included in the definition of insurer. Additionally, the definition of insurer excludes "foreign reinsurers." It seems contradictory that the insurer definition would specifically exclude foreign regulated entities, yet the licensee definition, through the inclusion of unauthorized insurers, would specifically include them. At the very least, the working group may want to consider aligning these definitions. For the avoidance of doubt, Lloyd's recommends adding the words "alien-domiciled reinsurers" to Section 3(V)(4) to make clear that reinsurers domiciled outside the United States are not subject to the insurer definition, just as is the case with foreign reinsurers, i.e. US reinsurers domiciled outside the adopting state.

## Section 7(C)

Section 7(C) of the Exposure Draft illustrates other challenges with deeming alien companies to be licensees. Section 7(C)(1) says that a consumer “may, but is not required to, consent to the... sharing of the consumer’s personal information [in] a jurisdiction outside of the United States.” Alien surplus lines insurers, such as Lloyd’s, are unlicensed entities in the US and consequently are not allowed to establish insurance operations in the United States. In other words, Lloyd’s is not allowed to establish an insurance operation in the United States in order to process a consumer’s personal information in this country. For Lloyd’s, the processing of such information must occur in the United Kingdom, where Lloyd’s is licensed to run an insurance business. Therefore, Section 7(C)(1) is not workable when the insurer is itself outside the United States.

But please note, even in the absence of this section, consumer consent and choice are still present. Consumers, of course, have the choice of buying insurance coverage from Lloyd’s in the first place. However, buying an insurance policy from Lloyd’s of London inherently involves sending customer information to the United Kingdom.

The proposed Section 7(C)(3) also highlights the challenges of creating a revokable consent process when the insurer is domiciled outside the United States. Section 7(C)(3) reads, “That once consent has been given for the collection, processing, retention, or sharing of consumers’ personal information in a jurisdiction outside the United States and its territories, a consumer may revoke consent at any time.” If a consumer’s insurance carrier is located outside the US, then a consumer’s revocation of consent would effectively be a mid-term cancellation of the policy because the non-US carrier would no longer be permitted to hold information about that consumer in order to service the policy. In other words, when the insurer is not located in the US, a consumer cannot both revoke consent under Section 7(C)(3) and maintain the insurance coverage.

In Lloyd’s view, the way to overcome the fundamental disconnect between the proposed consent for non-US processing, retention, or sharing of information, the desire for consumers to be able to retract consent at any time, and the fact the insurance company is itself based outside the US, is to remove licensees and third-party service providers based outside the US from the requirements of Section 7(C)(3) if those entities are themselves required to comply with the Act. The same language that Lloyd’s suggested be added to Sections 4(A)(5)(b) and 4(C) must be added to Section 7(C)(3) to accomplish this objective.

*If the licensee shares consumers’ personal information with a person who will collect, process, retain, or share consumers’ personal information in a jurisdiction outside of the United States and its territories, the following information shall additionally be included in any notice required by Section 6 of this Act. However, this subsection does not apply to the transfer of consumer’s personal information to a licensee or third-party service provider which is based outside the United States and is required to comply with the provisions of this Act.*

## Section 7(E) – Delegation of Notice Delivery

Section 7(E) is an important provision for unauthorized insurers. In Lloyd’s reading, Section 7(E) attempts to memorialize that the delivery of consumer notices can be either performed by the licensee or delegated to another licensee or third-party service provider that is authorized to act on the licensee’s behalf. This is an important provision for unauthorized insurers because in the surplus lines context the delivery of policy documentation, including notices, is handled by the surplus lines broker. It is critical that the ability to delegate notice delivery is clearly delineated.

In Lloyd's view, it is confusing to memorialize the ability to delegate notice delivery within Section 7, which is a section otherwise devoted to the *content* of consumer notices. Section 8 is a better home for the current Section 7(E) because Section 8 is entirely devoted to the *methods* of notice delivery. Lloyd's recommends moving the current Section 7(E) to Section 8 with following minor adjustment to account for its placement within a different section:

*The consumer notice obligations imposed by this ~~section~~ Act upon a licensee may be satisfied by another licensee or third-party service provider authorized to act on its behalf.*

### **Section 3(C) and Article V - Adverse Underwriting Decision**

The definition of adverse underwriting decision contained in Section 3(C) highlights another obstacle with deeming unauthorized insurers to be licensees. As previously mentioned, the Exposure Draft deviates from the typical NAIC definition of a licensee to include unauthorized insurers, also known as nonadmitted insurers, in its scope. At the same time, the definition of "adverse underwriting decision" in Section 3(C)(1)(e)(i) says that an adverse underwriting decision includes, "Placement by an insurer or producer of a risk with a...non-admitted insurer, or an insurer that specializes in substandard risks." In this framework, with unauthorized/nonadmitted insurers both a licensee and within the adverse underwriting regime, if a state were to adopt Article V, then surplus lines carriers, such as Lloyd's, would be obligated to notify their clients that by virtue of having Lloyd's coverage they have been subject to an adverse underwriting decision. This would be a perverse and punitive requirement, which is not supported in fact. Additionally, nonadmitted insurers are already required to provide notices that highlight for consumers the differences between admitted and nonadmitted coverage.

The obvious way to fix this problem is to remove unauthorized/nonadmitted insurers from the licensee definition in Section 3(X). However, even if the drafters pursue this option, Lloyd's encourages the working group to reconsider the proposed definition of "adverse underwriting decision" to ensure it is fit for purpose in 2023. Lloyd's rejects the suggestion that coverage provided by a nonadmitted insurer is in any way "adverse." Indeed, many consumers, regulators, and legislators would also not consider coverage with a nonadmitted insurer to be adverse, harmful, or a negative outcome. Securing coverage from a nonadmitted insurer is often the difference between a consumer either going without coverage entirely or procuring coverage from a state-backed residual market. In areas subject to hurricanes and wildfires, nonadmitted insurers, such as Lloyd's, provide an important source of capacity where admitted markets have pulled back. These nonadmitted carriers are providing a valuable service by providing insurance where others will not, and in so doing are helping to close the protection gap – something the NAIC has spent years trying to achieve and is one of its 2023 objectives. These nonadmitted insurers should not at the same time be subject to the pejorative label of an "adverse underwriting decision."

### **Section 13(B) – Presumption of Nondiscrimination**

Section 13(B) states that a rebuttable presumption of nondiscrimination and nonretaliation is created if certain actions are taken, which are "consistent with the licensee's filed rules, rates, and forms, and normal underwriting guidelines in the state." This provision is not workable for unauthorized insurers because these insurers do not file rules, rates, forms, or underwriting guidelines with state regulators. Again, the simplest way to remedy this issue to remove unauthorized insurers from the licensee definition.

**Private Right of Action**

Lloyd's would be remiss if we did not record our objection to the inclusion of an optional private cause of action in the Exposure Draft. This topic is far outside the remit of a regulatory, standard setting organization. Lloyd's recognizes that whether to include a private cause of action in privacy legislation is a key discussion point in many jurisdictions and has derailed many a privacy bill. However, rather than joining a heated and ongoing debate which is not going to be resolved by insurance regulators, we would encourage the NAIC to produce a model that adds value to the larger privacy discussion by leveraging and focusing on the NAIC's insurance regulatory expertise. We would suggest that the policy decision of whether there should be a private right of action for privacy and, if there is, how such a provision should operate is better left to policymakers in state legislatures.

Lloyd's appreciates the opportunity to offer these comments and would be glad to discuss them further with the Working Group.

Very truly yours,



Sabrina Miesowitz  
General Counsel



Timothy W. Grant  
Associate General Counsel



**MEDICAL PROFESSIONAL  
LIABILITY ASSOCIATION**

April 5, 2023

Chair Katie Johnson (VA); Co-Vice Chairs Cynthia Amann (MO) and Chris Aufenthie (ND)  
Privacy Protections (H) Working Group  
National Association of Insurance Commissioners  
1100 Walnut Street, Suite 1500  
Kansas City, MO 64106-2197

**Subject: Comments on Proposed Privacy Model 674**

Dear Ms. Johnson, Ms. Amann, and Mr. Aufenthie:

On behalf of the Medical Professional Liability (MPL) Association and its more than 50 medical professional liability insurer members, we would like to thank you for the opportunity to share our feedback on the working group's proposed consumer data privacy model (MDL #670).

The Medical Professional Liability Association is the leading trade association representing insurance organizations with a substantial commitment to the MPL line. MPL Association members insure more than one million healthcare professionals in the U.S.— physicians, nurses, dentists, oral surgeons, nurse practitioners, and other healthcare providers. MPL Association members also insure nearly 2,000 hospitals and 7,500 medical facilities throughout the United States.

The MPL Association supports the adoption of consumer data privacy policies that reflect the need to protect consumers from the unauthorized collection, processing, retention, and/or sharing of their personal information while recognizing the legitimate need for companies to use consumer data for appropriate insurance purposes. Such purposes include the provision of a full range of insurance services to meet its contractual obligations, the analysis of data to enhance future business practices, and compliance with all legal requirements. We recognize that balancing these competing interests is no simple task, and so we appreciate the working group's willingness to solicit feedback on Model #670.

With this in mind, we respectfully submit the following feedback with the understanding that additional modifications may be necessary depending on what changes are made to the proposed model following this initial comment period.

**Art. 1, Sec. 2. Oversight of Third-Party Service Provider Arrangements –**

The proposed model appropriately requires licensees to contractually require third-party service providers to comply with the model and the licensee’s own privacy practices. However, it would be inappropriate to require licensees to renegotiate all of their third-party service contracts immediately upon the enactment of a new privacy law based on this model. Instead, we would recommend including a grandfather clause that exempts existing third-party service contracts that are in effect at the time that privacy legislation is enacted. Alternatively, you may want to consider giving licensees a minimum of a two-year grace period to update all their third-party service contracts.

**Art. 1, Sec. 3. Definitions, Subsec. I. Consumer –**

The definition for “consumer” is overly broad, potentially subjecting insurers to regulatory scrutiny over matters not involving the insurer-policyholder relationship. As such, the definition should be limited to applicants, insureds, and beneficiaries.

**Art. II., Sec. 4. Data Minimization and Sharing Limitations –**

We applaud this working group for including language that allows licensees to collect, process, retain, and/or share a consumer’s personal information in connection with an insurance transaction as necessary, including for the servicing of any insurance application, policy, contract, or certificate, as well as for compliance with a wide variety of legal requirements. These paragraphs adequately address our members’ need to collect, process, retain, and/or share consumers’ personal information to accurately underwrite medical liability insurance policies and defend their insureds when claims arise.

**Sec. 5. Retention and Deletion of Consumers’ Information –**

We are pleased that Section 5 allows for the retention of consumers’ personal information for the servicing of any insurance application, policy, contract, or certificate, as well as for compliance with a wide variety of legal requirements, following the dissemination of an initial consumer privacy protections notice. This section adequately addresses our members’ need to collect, process, retain, and/or share consumers’ personal information to accurately underwrite medical liability insurance policies and defend their insureds when claims arise. Furthermore, we concur with the decision to not confer upon consumers the right for their personal information to be forgotten.

**Sec. 11. Access to Personal Information –**

We believe the timeframe permitted for responding to a consumers’ request for access to their personal information is unnecessarily limited, and may pose a burden on smaller insurers that lack the resources to turn around such a request so quickly. Instead, we propose a 30-day time period for the disclosures required under Subsection B(2).

**MPL Assn Comments on Proposed Privacy Model 674**

The MPL Association strongly agrees with the limitation of a consumer's right to access personal information that is related to a claim or civil/criminal proceeding, as indicated in Subsection G.

**Sec. 12. Correction or Amendment of Personal Information –**

Given the “long-tail” nature of MPL insurance, our member companies must collect and retain accurate information about parties (i.e., personal health information) to an MPL claim for claims processing, risk management, and quality improvement/patient safety purposes. Hence, we are pleased to see that the consumer right to delete or correct information in this section is accompanied by exceptions that allow a covered entity to deny such requests with an explanation of its need to retain accurate information to fulfill legitimate business transactions and comply with legal obligations. We also agree with the carveout of personal information necessary for a claim or civil/criminal proceeding.

**Art. V, Sec. 14. Adverse Underwriting Decisions –**

Section 14 gives insurers just ten (10) business days to share with a consumer the reasons for an adverse underwriting decision. Insurers need adequate time to investigate and compose formal correspondence that detail the reasons for adverse underwriting decisions. We would recommend giving insurers a minimum of ninety (90) days to respond to these requests.

**Sec. 19. Compliance with HIPAA and HITECH –**

The MPL Association is concerned about proposals that require MPL insurers to comply with overlapping privacy requirements that may complicate efforts to safeguard consumers' personal health information. While we are pleased to see this model provide a limited exemption to entities that already protect consumer information in accordance with the requirements for protected health information under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act, we believe a complete exemption is appropriate to avoid dueling data protection requirements.

**Sec. 26. Penalties and Sec. 28. Individual Remedies –**

The MPL Association strongly objects to the inclusion of language in Section 28 that gives states the ability to give consumers the right to bring forth a private cause of action for alleged violations of the privacy protections included in the model act. Additionally, this section unfairly holds the licensee responsible for the failure by a third-party service provider to protect personal information. Insurers must not be held responsible for the actions of those over whom it cannot exercise sufficient levels of control to ensure compliance with this model act. Instead, enforcement of data privacy legislation should be limited to civil penalties and/or injunctive relief for covered entities that fail to comply. While the penalties outlined in Section 26 are a good start, we would recommend amending it to include a tiered system of civil penalties based on a covered entity's past behavior and its adoption of corrective action.

In closing, the MPL Association appreciates this opportunity to provide constructive input to support sound, fair, and effective public policy as the working group refines this proposed model. Please do not hesitate to contact our Government Relations Department at 301.947.9000 or via email at [governmentrelations@mplassociation.org](mailto:governmentrelations@mplassociation.org) should you need any further information.

Sincerely,

A handwritten signature in blue ink that reads "B. K. Atchinson". The signature is fluid and cursive, with the first letters of the first and last names being capitalized and prominent.

Brian K. Atchinson  
President & CEO





April 3, 2023

NAIC Privacy Protections (H) Working Group  
NAIC Central Office  
1100 Walnut Street, Suite 1500  
Kansas City, MO 64106

Attn: Lois Alexander, NAIC Market Regulation Manager  
Via email: [lalexander@naic.org](mailto:lalexander@naic.org)

Dear Chair Johnson, Vice Chairs Amann and Aufenthie, and Members of the Privacy Protections Working Group:

The National Association of Benefit and Insurance Professionals (NABIP), which was previously known as the National Association of Health Underwriters (NAHU), appreciates the significant work the Privacy Protections (H) Working Group has completed in developing a new draft Consumer Privacy Protections Model Law. As an association of health insurance agents, brokers, and consultants, we believe protecting privacy is paramount both to our members and the consumers they serve.

We appreciate the time, energy, and consideration the members of the Working Group have put in to develop the model to date. Now that it is available for public exposure, we are engaging with our members about the contents of the draft. In the coming weeks, as you review the different sections of the draft with stakeholders and seek section-specific comments, we look forward to providing you with meaningful feedback based on data-gathering with our members. In addition, we greatly appreciate the Working Group's stated intention to hold an in-person meeting in June with stakeholders regarding model development.

Based on initial analysis of the new draft, we do have some significant specific concerns. First, rather than a simple revision of the existing model legislation, this new draft represents a large departure from the current model, which is the basis of law in many states. Additionally, while this proposal provides a compliance safe harbor for Sections 4-8 of the draft, provided a licensee complies with the federal HIPAA/HITECH privacy and data security requirements and meets other criteria, there is no such safe harbor for compliance with other sections of the draft act, even though those sections are also duplicative of HIPAA/HITECH. Dual regulation of this type is confusing and cumbersome for both licensees and consumers. Further, we



have concerns about the private right of action allowed by this model, and feel that the regulatory requirements are not always appropriate for small independent insurance producers and agencies.

We look forward to communicating with you more about the proposed changes to the model act in the months ahead, and truly appreciate your willingness to consider the views of all stakeholders. If you need any additional information or have any questions, please do not hesitate to contact me at (202) 595-0639 or [jtrautwein@nahu.org](mailto:jtrautwein@nahu.org).

Sincerely,

A handwritten signature in black ink, which appears to read "Janet Stokes Trautwein". The signature is written in a cursive style with a large initial "J".

Janet Stokes Trautwein  
Executive Vice President and CEO  
National Association of Health Underwriters

**NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS  
PRIVACY PROTECTIONS (H) WORKING GROUP**

***New Consumer Privacy Protections Model Law #674  
Initial Exposure Draft (2/1/23)***

On behalf of the National Association of Mutual Insurance Companies (NAMIC)<sup>1</sup> members, thank you for the opportunity to provide these comments on the February 1, 2023 exposure draft of a new Consumer Privacy Protections Model Law #674 (exposure draft). NAMIC appreciates that the Privacy Protections (H) Working Group (PPWG or Working Group) allowed two months for review of the initial exposure draft and is grateful for the upcoming open meetings (virtual and in-person) regarding the language of that model.

Before turning to specific wording suggestions, the purpose of this statement is to highlight serious concerns with the initial exposure draft in terms of: (1) framework, (2) workability (including necessary exceptions such as those reasonably anticipated in context of a consumer relationship and/or without which the day-to-day business of insurance could not get done), and (3) exclusivity. Respectfully, the distance between a functional consumer privacy protection regime and this exposure draft is significant. These comments seek to showcase possibilities for meeting regulatory objectives of providing consumers more choices with respect to personal information while also making the system feasible for licensees.

**(1) FRAMEWORK: Build on a solid privacy foundation. Avoid disruption.**

*Introduction*

As architects of a new model law, the PPWG seeks to design a set of privacy responsibilities and options that will serve consumers (along with regulators and licensees). As the PPWG constructs Model #674, we urge the Working Group not to disrupt the strong foundation on which the current privacy system is built. Rather, through some design revisions, the exposure draft could support consumer privacy by adding onto the current structure's strong foundation and sensible layout.

We strongly suggest that the PPWG build on the existing framework which is premised upon notice, not consent. Rather than creating a distinct privacy framework, the Working Group should build upon GLBA (and not be inconsistent with CPRA) by giving consumers certain choices by "opting out" in addition to notice. This initial exposure draft would become the first law to be premised almost entirely on consent – consent to marketing, to additional permitted transactions (which encompass day-to-day business operations), to where data can be processed, to research and analytics. The potential impact to insurers' business with limited potential benefit to consumers must be evaluated closely.

<sup>1</sup> NAMIC Membership includes more than 1,500 member companies. The association supports regional and local mutual insurance companies on main streets across America and many of the country's largest national insurers. NAMIC member companies write \$323 billion in annual premiums. Our members account for 67 percent of homeowners, 55 percent of automobile, and 32 percent of business insurance markets. Through our advocacy programs we promote public policy solutions that benefit NAMIC member companies and the policyholders they serve and foster greater understanding and recognition of the unique alignment of interests between management and policyholders of mutual companies.



While generally speaking a licensee would not necessarily expect to be compliance-ready the day any model is drafted, in looking at this initial exposure draft and even assuming ample time before it would take effect, its approaches just could not be implemented practically given its business-altering treatment of marketing and international sharing. Imposing a consent-based framework for communicating about new/additional products or services, engaging in research, and any data sharing outside the U.S. would appear to: be impracticable to implement, slow growth, hinder innovation, add costs, put insurers at a competitive disadvantage compared to other industries, and reduce consumer awareness of risks and insurance products/services to protect from such risks. The potential disruptive consequences are very significant.

#### *Marketing Treatment Under the Exposure Draft & Need for Revision*

The initial exposure draft creates an opt-in framework requiring explicit consent for all kinds of marketing, including: an insurer marketing its own products to its own policyholders, marketing through an affiliate, or under a joint marketing agreement. It appears to restrict communications about risks, products, and services, despite coverage gaps being a recurring topic at the NAIC. Our concerns about this approach are multifold:

- It would be more restrictive than any other privacy law. State privacy laws and Title V of GLBA (as was built into Model #672 and adopted across the country) do not require consent before marketing. Even CCPA – widely deemed the most aggressive privacy law in the U.S. – largely created an opt-out framework.
- It may create a competitive disadvantage for insurers compared to other industries.
- It ignores the public benefit from insurance and from wide adoption of insurance products. Marketing increases consumers' awareness of financial risks and ways to address them and it extends insurers' reach in raising such awareness. The initial exposure draft model ignores these public benefits by making it increasingly difficult to reach consumers where they find information.
- In the insurance context, there are longstanding and successful legal frameworks which appropriately balance relationships and the importance of data for consumer and licensee alike. These frameworks are consistent with consumer expectations for data use, having set the status quo for decades.
- It ignores the current state of insurance regulations related to marketing. Model #672 was largely integrated into most states during the process of implementing GLBA. It includes a set of exemptions for business functions that preserve a licensee's ability to share information in order to conduct the business of insurance. Importantly, it does not restrict any disclosure of nonpublic personal information with affiliates and it allows licensees to share nonpublic personal financial information with unaffiliated financial institutions subject to a joint marketing agreement. The existing regulatory environment does not require consumer consent to be in such a joint marketing agreement. The initial exposure draft flips the current state on its head and suddenly would require consumer consent for what has been an accepted practice for decades.

To be clear, the exposure draft's requirement that insurance companies obtain consent prior to marketing would decouple insurance regulation from longstanding GLBA and financial services norms, disadvantaging insurance products as compared to other financial products and services. The limitations may have very significant financial impacts for companies and the financial security of the consumers our member companies serve.



### *Joint Marketing's Value*

For the purposes of this letter, it may be useful to provide a greater understanding about insurers engaging in joint marketing with other trusted financial institutions. Under GLBA and its regulation, financial institutions must undertake certain privacy protections and security safeguards to share and use nonpublic personal information in joint marketing programs. Financial institutions must enter into a contract for the joint marketing program which limits the use of shared nonpublic personal information to the joint marketing program. In addition, financial institutions under GLBA must also provide notice to individuals that their information will be shared for joint marketing.

By collaborating and contracting with other financial institutions in marketing arrangements, there is a level of mutual confidence that the respective financial institutions share an interest in a consumer's financial well-being and that they are subject to similar regulatory and legal requirements to protect nonpublic personal information as they are subject to GLBA, including the need to provide "administrative, technical, and physical safeguards." (See 15 USC 6801(b).)

In financial services, trust is critical to consumer decision making. Particularly in a joint marketing context, financial institutions are incented to maintain trust in all actions, including use of consumer data, as any violation of trust is sure to result in lost customers and partner organizations. Joint marketing serves a valuable role in extending the reach of smaller and mid-size insurers to consumers with whom they do not have a direct relationship. Further working with a trusted financial institution may be less intimidating to those who need assistance with achieving financial security the most, through relevant marketing and increased awareness of available insurance options.

To require that consent be secured in advance of marketing would frustrate the very purpose of this arrangement and it would drain resources of smaller financial institutions. In many cases, joint marketing efforts have been long established and are essential to some insurers' business models. The negative impact of an opt-in would be significant. Consider what it could mean to stop the growth of such insurers as well as to suppress convenient outreach, including to middle-market and underserved consumers. Would insurers be required to turn to more expensive and less efficient forms of mass media marketing? Would consumers receive more marketing requests and/or more product information that is not relevant?

Mindful of these costs, let's revisit the broader policy objectives of insurance regulation: for consumers to understand their risks and to be informed so they can decide whether/how to insure appropriately while also being able to direct their financial institution consistent with their preferences to the extent choice is provided under the law.

### *Direct & Affiliate Marketing's Value*

To extensively curb communication about insurance products and services does not heighten awareness of risk or expand informed decision-making around insurance products and services. In times when so much emphasis is being placed on coverage gaps, it seems counterproductive to shrink communications – through a licensee or its affiliate – about risks and coverages. To require prior consent for marketing presents too many serious logistical and public policy challenges. In moving forward, it is crucial for the Working Group to resolve this issue.

Consider the situation of informing a policyholder of additional coverage options. Here are some examples of potentially challenging situations as drafted under the initial exposure draft:



- ✘ If a homeowner installs a pool, it may be helpful to educate them on the value of additional insurance/coverage options/products that may be beneficial. This would not be permitted without first obtaining permission.
- ✘ If a consumer has an auto policy, a licensee first would need to obtain express permission before telling a consumer about homeowners insurance offerings.
- ✘ If a consumer has homeowners coverage, a licensee first would need to secure an opt-in from a consumer before sharing that she may have a gap in coverage relating to flood exposure.
- ✘ If a consumer has auto and homeowners coverage with a licensee, it might be read as prohibiting conversations about umbrella coverage without obtaining consent first.

A system under which all consumers are dispossessed of this insurance information – unless they adhere to the initial exposure draft’s proposed new written formalities – is not in most consumers’ best interest.

### *Marketing & Compliance with Federal Laws*

The new privacy model would not be in a vacuum. Consider the federal laws dealing with marketing that apply countrywide to all businesses, including insurers. One example of an opt-out model is under the federal CAN-SPAM Act, which has largely worked well at requiring reputable companies to allow consumers to easily opt out of commercial emails (to “unsubscribe” from future emails) and at setting forth other messaging principles to apply to commercial emails. The one U.S. exception to an opt-out regime for marketing is the Telephone Consumer Protection Act (TCPA), which is very specific to telemarketing involving automated telephone dialing systems (ATDS). In other words, TCPA takes a more surgical approach on restrictions by focusing on the delivery mechanism, rather than attempting to require opt-in consent for all marketing. These existing laws and the licensee practices built around complying with them may give the Working Group additional comfort about existing consumer protections for these forms of marketing.

### *Research/Actuarial*

There is anxiety around what is meant by research (and actuarial studies) and what exactly would require prior permission. The initial exposure draft is unclear in its definitions and what specifically it would permit if consumer consent were granted (and what it would prohibit). Regardless of those definitions and of the scope, it is important to recognize that today U.S. laws do not currently require consent for research, aside from a medical context. And there are valid reasons why research is excepted from a consumer opt-out otherwise. Efforts are being made to better understand what may not be deidentified that would be a concern. One item that comes to mind is actuarial analysis which may not always be related to rating that particular insurance transaction. Also, where might analysis relating to underwriting fall? Other internal analysis? It is important that information be credible and not weakened; it serves a critical role in the insurance ecosystem. Consider the potential negative consequences of an opt-in: potentially skewing data (reduced sample size and/or introduced selection biases may have statistical impacts).

### *Operational Considerations & Alternatives*

As the NAIC considers what mechanism to put in place for a consumer to use to make choices regarding certain personal information, consider its impact and the broader situation. In looking at the general privacy laws (encompassing transactions that do not have the same essential data needs as insurance and where there is not the same type of relationship) for areas where a choice mechanism is provided, the vast majority of the U.S. comprehensive privacy law requirements are structured as opt-out. The exposure draft’s opt-in framework would trigger a major operational undertaking well beyond changing privacy notices. Insurers would need to build processes/repositories to manage consents. This would demand significant time and resource commitments,



imposing technical as well as financial burdens. (And as mentioned earlier, in the context of marketing, research, and sharing data outside the U.S., it would be implausible.)

The objective of protecting consumers who wish to restrict information-related activity can be met under either an opt-in or an opt-out. No greater privacy protection is afforded to an individual wanting more restrictive data handling under either approach. Under both approaches the individual consumer controls the decision. The difference is the default. However, an opt-in approach offers fewer choices to consumers because it assumes that consumers value restrictions over the benefits of product and service variety, innovation, and/or ease of use. Not only may an opt-in be more costly to administer because it would require companies to obtain consent, but consumers may perceive it as more intrusive due to increasing licensee contacts with the consumer in an effort to secure consent. As discussed, especially in the context of insurance, an opt-in could have meaningful negative consequences.

Returning to construction analogies, sometimes it's better to build onto an existing structure than to demolish and rebuild. Today insurers have an infrastructure in place to handle opt-outs. That framework could be leveraged to handle additional requests (though even that modification would require operational effort to implement, especially for licensees not doing business in California). Even if the Privacy Protections Working Group wants to expand the scope of Model #672 beyond its primary focus of privacy notice and an opportunity to opt out of certain sharing with nonaffiliated third parties, the basic concept and structure of that model does not need to be obliterated. Rather, because it outlines a framework – for privacy notice, option (opt-out) notice, limits/restrictions/requirements, exceptions, and more – it could be adapted by adding expanded notice content and consumer requests (access, correction, etc.). And if the Working Group elects not to use that model as a starting point, it still may be a helpful resource as the Working Group considers how to address marketing in a fair and reasonable way.

#### *Data Direction and Cross Border Restrictions*

As currently written, Model #674 would be designed to let consumers direct the location of licensees' operations and third party service providers. This is incredibly problematic as a disruptor and unworkable outlier that ignores modern realities.

A cross border restriction could introduce significant challenges for global companies. The current system should be preserved – the initial exposure draft would overturn decades of structure. This wording currently in Sec. 4(A)(5) of the initial exposure draft would mandate that an insurer obtain consent from the customer if it shares or processes customer information outside the United States. This is a very significant restriction to insurers and their ability to use offshore third-party service providers or to use a company's own operations located in another country. Some insurers have already invested substantial resources and effort to transform critical functions using offshore vendors. These functions include customer care and engagement, finance and account management, business analytics, and IT security. Further, these operations/TPSPs are integral to efficient policyholder service. For some licensees, this may mean work (and responding to policyholders) can occur around the clock – removing geographical diversity may possibly extend wait times for claims processing and other services. Today's international operations/TPSP may also help smooth and mitigate disruptions, consistent with business continuity planning. Requiring consent to move data out of the U.S. would mean company IT teams in other countries could not assist with the U.S. business. Replacing all offshore vendors is not realistic and may impact both the customer experience and costs.



Parallel operations would be impracticable. The opt-in included in the initial exposure draft would seem to expect an insurer to replace or duplicate third party service providers to accommodate for those customers who do not provide consent – parallel staffing/vendors (across many services and functions) may be unworkable and cost prohibitive. Considering the volume of policyholders, building to parse between those who opt-in seems to present obstacles (especially when revocation could occur at any time). Indeed, no state law comes to mind as imposing this kind of restriction. A state passing a model with this approach would present a difficult challenge.

As drafted, the initial exposure draft seeks to impose a limitation on transferring information outside of the United States, a limitation that is contrary to the free flow of data and prohibition on data localization policy positions and commitments adopted by the U.S. in its trade agreements, at the G7, and in its financial regulatory dialogues. The position put forward in the initial exposure draft to limit the transfer of data outside the U.S is also inconsistent with positions taken by global regulatory bodies such as the Financial Stability Board (FSB) and the International Organization of Securities Commissions (IOSCO). The free flow of data is not contrary to ensuring data privacy or security. Protecting consumer information is not dependent on the location of where data is stored or processed, or the location of the infrastructure supporting it. Rather, protection is a function of the technologies, systems, and internal controls put in place by the companies handling the personal information to protect the data.

The position in the initial exposure draft is not only inconsistent with U.S. policy positions, it is contrary to the positions adopted by U.S. peer countries/jurisdictions such as the U.S., EU, UK, Singapore, Japan, and Australia. These governments support the free flow of data, including for personal information, and the need to prohibit data localization requirements while at the same time maintaining privacy frameworks. The European Union's General Data Protection Regulation (GDPR) does not impose prior consent as the only basis for legitimate overseas sharing/processing/housing data within different countries. Singapore, Australia, Japan, and the United Kingdom maintain privacy frameworks without restricting the free flow of data outside their territories. These countries, like the United States, also have entered into free trade agreements that include commitments to the free flow of data and the prohibition on data localization.

In summary, no ability to direct – opt-in or opt-out – is appropriate for governing a TPSP/operation location. Note that today TPSPs (including those that are not domestic) are already subject to cybersecurity oversight under Model #668 and other contractual provisions. If the NAIC feels that it must address the topic of sharing data outside of the U.S., it may be that it could approach this issue through disclosure only (as a notice item, though that may lengthen notice and present other potential drawbacks). Given all these concerns, it is essential to remove data location direction from any model before moving forward.

**(2) WORKABILITY: A new model is more workable when it aligns some of the timeframes and wording with existing laws, contains flexibility without being overly prescriptive, preserves exceptions, remains focused on core privacy matters, transitions prospectively and with a delayed effective date, and offers helpful models/templates and safe harbor wording.**

Many of the workability issues with the initial exposure draft become evident because (or arise due to the fact that) a new model, applicable only to the insurance sector, would not be adopted in a vacuum. Several examples, though not an exhaustive list, are highlighted below.





## Existing Privacy Laws

As was mentioned with regard to the framework question of opt-in/out, the initial exposure draft differs from and goes further than existing requirements. If/where the new Model #674 does not align with existing privacy laws, it increases compliance burdens unnecessarily. Consider several examples.

Notice Frequency & Annual Notice Compliance Deemer – Unfortunately, Section 6(C) would eliminate the 2015 FAST Act relief (which included an amendment to GLBA (see addition of Sec. 503(f)) involving an exception to the annual notice requirement). Not only did federal financial regulatory authorities make this corresponding change, but the NAIC (via the Gramm Leach Bliley Act Annual Privacy Notices NAIC Model Bulletin) and the vast majority of states (we understand the current count to be 47 states) did as well. Not being required to send the notice when two conditions were met – (1) previous notice had been provided to the consumer; and (2) practices disclosed had not meaningfully changed – has meant efficiencies and not spending money for this paper distribution. To share a sense of financial impact, one mid-sized member company reports that upon passage of the FAST Act annual notice obligation change, their assessment quantified an expected savings of \$450,000 per year (in 2015 dollars). The potential backsliding on this progress and returning to requiring volumes of unpopular repeat customer notices has prompted resounding opposition. Today, with additional prominence of online consumer engagement and with strong support for improving environmental/climate conditions (and in an ESG context), there is pressure for reducing the amount of paper sent. The initial exposure draft’s approach to annual notices in these situations would be a step back. If the Working Group favors reimposing this requirement despite its drawbacks, we ask for a discussion about whether online posting could suffice for compliance. Consumers do not need to receive repeat copies of identical notices.

Exceptions - Given the important role information plays, insurance regulators have a history of recognizing exceptions for operational and other reasons. As the Working Group continues with its drafting, the question of whether any of the historic exceptions will be disallowed in some or all situations is essential to discuss. This may require a mapping exercise to account for the exceptions from existing Models #670 and #672, GLBA, and CCPA. In addition, organizing the model so the exceptions are all in one section (and then indicating which ones correspond to notice, opt-in/out, and the various requests) may facilitate dialogue around them, aligning the requirements, and aid compliance. Regardless of how it is accomplished, the importance of any new model including all the needed exceptions cannot be overemphasized.

Notice Content – To take just one example, where California mentions “categories” and many insurers have expended significant effort to get into compliance with that state’s law, it would be appreciated if the PPWG could take a similar approach. Beyond consistency, things like disclosing “categories” of sources rather than a list of them will be more digestible by the consumer (rather than a list out of context) as well as more operationally feasible. Overall, the initial exposure draft goes further than any existing requirements based on the types of personal information licensees must disclose to consumers.

Consumer Requests & Disclosure of Sources / TPSPs – Under California’s comprehensive consumer privacy protection laws and NAIC Model Law #670, as well as state consumer privacy protection laws, many insurers have processes in place to provide consumers with and ability to request access. The initial exposure draft goes further by adding prescriptive elements, such as identifying and disclosing every source of personal information and every person or entity to which personal information was shared (e.g., from the auto body garage to the cloud service provider at hosts the claims system). Large licensees use many service providers to properly and securely service consumers and disclosing each of these service providers to consumers could add unnecessary length to the already lengthy response to consumers’ access requests. Most importantly, disclosing specific service providers to consumers could lower the security posture of licensees, since responding to these could reveal the exact type of equipment or systems that are being used by the licensee. Licensees should generally only be required to disclose categories of service providers that are used. This more reasonable disclosure



reduces the length of the disclosure and does not jeopardize the security posture of licensees, while still ensuring that consumers are aware that their personal information is being shared for specified purposes.

Timing for Request Acknowledgement and Response – The initial exposure draft would mandate that a request be acknowledged in only five business days and that such request be responded to within fifteen business days. These timeframes would be too short. In terms of the acknowledgement, ten business days would be more manageable and would be consistent with CPRA. Those licensees required to comply with CPRA in California would already have recently implemented for that time period (although note that many licensees have not had to so implement). With respect to the response, understand that CPRA (Sec. 1798.130(a)(2)(a)) allows for 45 days with an ability to extend an additional 45 days in certain circumstances. It may take time to search for responsive data and take action on it. (Insurers are contending with legacy systems and even within 45 days some report that it would not be feasible and indicate that 90 days would be more reasonable.) There is no need to treat insurers differently from other businesses for purposes of these acknowledgements/responses.

Additional Notice Triggers - The matter of notice volume concern is also exacerbated by the way the initial exposure draft may handle independent agent quoting and the need to supply a notice to former consumers that no future notices will be sent. These are examples of novel approaches that do not appear in other laws today; we urge the Working Group not to create additional times/triggers requiring that notice would need to be provided. This is inefficient and indeed, taken as a whole, may have the unintended consequence of causing consumers to have notice fatigue.

A new privacy model put forth by the NAIC should be allow for also being consistent with existing privacy frameworks. Harmonization with existing frameworks will be extremely helpful in reducing unnecessary compliance burden. Overall, the policies and procedures proposed should be less prescriptive and allow flexibility for licensees to account for the multiple existing privacy frameworks and various regulatory requirements to which licensees are already subjected. Many insurers aim to develop holistic programs, appropriate for their size and their business risks, that meet all their legal and regulatory requirements. This is much easier where there is flexibility and harmonization.

#### *Data Minimization and Retention/Deletion*

While some insurers already comply with portions of the initial exposure draft, it appears to seek to add prescriptive elements that are incredibly burdensome. These prescriptive elements are not likely to reduce consumers' privacy risks and could put the insurance industry at a disadvantage compared to other GLBA-regulated industries. One such example relates to data minimization, which would be done in a manner that goes further than any existing requirements. Indeed, concerns have been raised about the possible impact of the initial exposure draft on integrated financial services companies, licensed insurers, that also offer non-insurance products to address financial risk and consumer financial planning demands. Other financial institutions without insurance operations are not subject to the unusual approach outlined in the exposure draft; they would seemingly be better able to meet this consumer demand. As the drafting process moves forward these kinds of unintended consequences should be considered.

Licensees have created and maintained record retention schedules for many years that specify the period of time data must be kept and when it should be deleted. There are many laws governing these requirements. For example, as required by laws like the California Online Privacy Protection Act (CalOPPA), one insurer points to having long made an online privacy notice available to consumers and engage in business practices in compliance with this notice, as required. Within this online privacy notice, such insurer makes a general statement regarding retention needs and purposes.



The initial exposure draft goes further than existing data minimization practices because it requires deletion of personal information within 90 days after its use has been fulfilled. Secure deletion of information is a complex activity for a large, sophisticated entity that has thousands of interconnected systems. As written, it raises many questions. Is the use of the data fulfilled when the claim is closed? Licensees cannot delete the data when the claim is closed because of market conduct exams and potential litigation. And perhaps even if the use of the claims data is fulfilled, there may be accounting or claims trending reports that may require the information. A more precise statement would be that the data must be deleted in accordance with the company's record retention schedule and legal hold process. Most companies have a process in place to do this already but not on a 90-day cadence as suggested by the initial exposure draft. The Working Group should consider the complexity of the activity and use less prescriptive terms such as, "deletion shall occur after a commercially reasonable amount of time." The 90-day requirement is overly prescriptive and because it cannot account for particular situations and complexities, it should be replaced with an alternative that does not specify a certain number of days.

### *Third-Party Service Provider Contracts*

Because today licensees already are required to have oversight of third-party service providers under cyber Model #668, there should be flexibility as to the timing and less specificity as to the content of third-party contractual language. Consider the volume of agreements. Licensees may use hundreds or even thousands of third-party vendors to provide supporting services. Consider how this works in practice. Updating contracts is a massive project to manage. It involves more than just drafting new provisions. Administratively it involves outreach to each vendor, tracking, follow-up, etc. And this is not a hypothetical matter – licensees may have recently needed to revise contracts to address cybersecurity (as required under Model #668). Securing modifying terms mid-contract may be difficult – vendors may not have an obligation to renegotiate mid-term and some contract may be expected to be in place for a more extended period of time. With this in mind, the Working Group should consider several process-oriented revisions to the initial exposure draft, including things like being prospective only to contacts entered into after the effective day, the reasonability of "good faith efforts," and/or allowing for an additional extended time before these requirements would be required to be put in place. Recall that recognizing the contract-related challenge, when GLBA was first implemented, the effective date provision incorporated grandfathering contracts to allow for a longer time horizon to address existing vendor contracts (also refer to Models #672 and #668).

In addition to process, the initial exposure draft also would indicate specific content to be incorporated into contracts. This is problematic for several reasons. First, depending on the contract and the TPSP, requiring a third party to comply with the Act or to "abide by the provisions of the Act" may be a challenge. Reference to each state's laws or to a model may pose a problem as those change (and after this model is adopted, they may be changing even more for a period of time). As drafted, this would seem to require TPSP to comply with every provision of the model. But not all aspects of the model relate to the TPSP obligations. For example, they would not provide notice. While they could be directed more narrowly to wording similar to "abide by requirements consistent with applicable provisions this Act," that may assume that every TPSP is focused on the industry. Instead, as new contracts are put into place, it may be more effective to point to the particular expected actions and the purpose of the agreement for TPSP services. Second, thinking practically, third parties may not want to review each and every licensee's individual privacy policy. Requiring a third party to "abide by the licensee's own practices" could be difficult for vendors with many clients (including some across different industries). Some TPSPs may not be focused on the insurance industry; they may also have clients in other businesses. Further, large vendors may not accept modifications from insurers. Instead, again, as new contracts are put into place, it would be more effective to point to particular expected actions and the purpose of the agreement for TPSP services. Overall, this is another section of the initial exposure draft that would benefit from additional flexibility.



### *Adverse Underwriting Decisions*

Notices unrelated to privacy are best considered outside this model. Indeed, both the NAIC and NCOIL have had recent efforts relating to transparency. If the NAIC wishes to deal with additional notice requirements, it should conduct thorough research to catalog all of kinds of notices, legislative options available to states, and have a robust dialog dedicated to that topic outside of the privacy model.

From looking at the initial exposure draft, it is clear that there is not a common understanding or consensus around the term's meaning. For example, the Section 14(A) Drafting Note list contains items that should not be included. Specifically, consider that some of these items are not underwriting decisions. Also note that the general understanding of base rate is that it does not relate to a particular individual's personal information or individual risk. Importantly, this all highlights that not only is this issue a departure from the core privacy issues, but it is challenging and needlessly makes a complex model even more complicated.

Although provisions relating to "adverse underwriting decisions" were contained in Model #670 (and in a minority of states), it should not be carried forward (even as optional) because many state legislatures have enacted laws with different (and what might be overlapping) notices since the 1980s when that model was created. The vast majority of states have credit scoring laws in place (based on the NCOIL Model) that require adverse action notices. And this is not the only kind of consumer reports with notice requirements. States have the ability to act specifically to require notices relating to claims history information (and some states have enacted NCOIL Model on that issue). Additionally, states have a variety of all kinds of other notices including premium increase notices and conditional renewal notices. For several reasons, it is worthwhile to remove the adverse underwriting decision aspects of the exposure draft.

### *Transition: Effective Date & Implementation*

The kinds of changes – to notice content and timing, processes, specificity around request responses/actions, contracts, etc. – contained in the initial exposure draft would be sweeping. To comply, those changes must apply on a go-forward basis to transactions, data, consumers, contracts, etc. after the effective date(s). And there would need to be staggered effective dates to allow for implementation of different portions of the model.

We ask that regulators not assume that licensees all would be ready to implement in the near term. Because insurers are subject to laws in different jurisdictions, while some licensees may have already made some of the changes, for others who are not subject to some of the existing laws, those requirements would be new. For example, some regional or single-state insurers may not do business in California; their practices today may not be built around that state's law. Further, there are many provisions in the initial exposure draft that are completely novel. No other jurisdiction or sector has them in place today. If the Working Group decides to proceed with those, all licensees may need ample time for implementation.

Recall that GDPR was in development over a long period of time, it appears the draft proposal was released in 2012, some general agreement may have been reached in December 2015, it was adopted in April 2016, and enforcement began in May 2018. Even into 2019, news reports appeared to indicate that compliance challenges continued. Again, we would like to emphasize the importance of allowing for adequate advance time before the effective date. Some of the proposed changes would be extremely complex. This necessitates delayed implementation and possibly forthcoming optional model wording (consistent with the law) throughout the implementation process to facilitate compliance. Specifically, we believe that the timeline should be similar to the 2-5 years that was afforded under GDPR. Even within that timeframe, a prospective roll-out period setting forth different dates for different provisions sets-up a more measured approach to undertaking such a significant endeavor.



Finally, the Working Group should consider what the transition process would look like if one or a few states were to adopt a new model. Some licensees may report that it may not be operationally feasible to integrate or streamline notices. To ensure compliance with the legal/regulatory requirements, a licensee may feel compelled to send multiple notices to consumers. If there is no ability to use the federal model form, this problem could be exacerbated.

### *Model Language and Forms*

When it comes to notice content (and perhaps other aspects of a Model #674, such as acknowledgements, etc.) we urge the Working Group to offer optional compliance aids that may prove helpful in providing some additional certainty. Indeed, going through the exercise of drafting a model notice, to get a sense of what a consumer might receive, may be instructive for the Working Group. This experience was helpful in California. Many of the notice content requirements contained in the initial exposure are similar to the notice initially proposed by the California Privacy Rights Act (“CPRA”). It was approximately 10 pages in length (excluding lists of sources of personal information and disclosures to third parties). Upon reviewing public comments, the drafters of the CPRA ultimately elected to remove requirements to list every third party to which personal information is disclosed, citing operational infeasibility as the rationale.

Importantly, we urge the Working Group to include the ability of licensees to continue to allow use of a Federal Model Privacy Form, as was done in Appendix B of Model #672, for those who elect to follow it. Today, some licensees choose to provide consumers with the federal model form notice that provides a variety of important information to consumers in a format that is easily digestible. And it has the benefit of being uniform with other GLBA-regulated financial institutions. We strongly recommend the NAIC consider coordinating with federal GLBA regulators so that licensees have the option of sending consumers notices that are consistent in appearance and format.

The model law would require more detailed and lengthy notice, which could result in less informed consumers because average consumers may disregard lengthy text-heavy legal/compliance documents. The initial exposure draft would send consumers more than what is currently required by today’s laws. This should be considered (as outlined above) and the Working Group should also strongly consider how to continue to allow licensees the ability to use the Federal Model Privacy Form.

Further, there are numerous aspects of the initial exposure draft’s notice requirements that relate to raising awareness of a consumer’s ability to make certain requests. Because these aspects are not licensee-specific disclosures, they would be especially appropriate for brief regulator-generated safe-harbor wording. Even for the other notice/communication items, it may be useful to include optional sample clauses and examples, as was provided in Model #672 (as well as a short form notice), as useful operational guidance for licensees during implementation.

### *Delivery & Meeting Consumers Where They Are*

As we get further into the twenty-first century, it is clear that consumers’ preferences around technology have changed. Therefore, web-based posting of privacy policies should be allowed (with an additional alternative available for those not having or not wishing to use the online material). This is a common-sense efficiency that benefits everyone and we ask the Working Group to consider making such a change.

### **(3) EXCLUSIVITY: Develop stable, single, and certain standards through exclusivity.**

#### *Insurance Regulators as Sole Authority*

It is essential that any model make it clear that insurers subject to its provisions are not simultaneously subject to layers of potentially differing legal requirements. Avoiding dual regulation with other agencies/authorities is essential. When licensees are subject to multiple requirements, what needs to be done is much less clear and compliance becomes more difficult. It also may mean more confusion for consumers. For this reason, a “not inconsistent with” type way of drafting to address conflicts with other state laws is not strong enough in this setting. Rather, any model should form the exclusive standards and requirements applicable to licensees for data privacy.

Insurance departments know their licensees. Regulators are responsible for regulations and for rulemaking. Regulators scan for compliance – between monitoring for flags raised through complaints and market regulation/conduct reviews – to be aware of licensee practices. And they enforce the insurance laws; under this Act regulators would have strong enforcement authority. The context of insurance – the need for data, the business relationship with consumers, and the importance of understanding risk accurately – makes it unique and appropriate to be governed by their functional regulator (and not by general laws or by litigators).

#### *Private Cause of Action*

It is essential that any model avoid uncertainty, debate, and litigation prompted by a having private cause of action option in the model. The issue of a private cause of action falls within a broader context of ensuring that licensees have single certain standards governing their privacy practices and obligations. No private cause of action should be suggested, even on an optional basis, in the new exposure draft. While “individual remedies” were included within the old Model #670 which was adopted in a minority of states, this is an exception for an NAIC model and extremely problematic for the NAIC to include such provision. More broadly, litigation has not generally been a component of the general privacy laws. It is not contained within the European Union’s GDPR or in California (other than for breach, which is not the subject of this draft). To include this in an insurance sector-specific approach would be out of step.

Private lawsuits could erode uniformity and distract from the goal of meaningful and real privacy protections. As indicated above, avoiding multiple layers of oversight – with potentially inconsistent interpretations – is essential. And it may be that drafting the model to include a private cause of action serves to encourage litigation when issues might be non-material or not harm policyholders. By allowing separate litigation, the NAIC risks courts substituting their own judgment for that of the NAIC and state regulators who have specialized knowledge in the area and of the licensees. Uncertain legal and regulatory requirements make a business environment more costly and unpredictable, at best.

To underscore the point, insurance regulators themselves are the ones best able to assess patterns of privacy-related practices and address any noncompliance efficiently to protect all consumers. The NAIC should focus on protecting insurance consumers through corrective action. A litigation-oriented regime picks winners and losers, removing regulators from their objective regulatory role. Therefore, by the NAIC proceeding with the Section 28(A) approach, it would make it clear that no private cause of action is created under the model and it would be asserting insurance regulators’ authority on this issue. We urge the NAIC Privacy Protections (H) Working Group to prioritize valuing exclusivity and making it clear that there is no private cause of action arising from a modern NAIC privacy model.

\* \* \* \* \*

Kindly understand that these comments are preliminary in nature as members assess the draft wording going forward. And language will continue to evolve in important ways. The business of insurance does not occur in a vacuum – there are many aspects to the business that must be considered carefully to avoid licensee disruption and consumer confusion/harm. This includes thinking through treatment of reinsurers under any model as well as careful consideration of exceptions and other operational matters. The practical implications of the operational requirements will depend both on the big picture concepts as well as the specific wording. Because data is essential to an insurer being able to better understand and more accurately underwrite risks, the ability to access necessary information and to comply with other laws regarding information will remain an important component of NAMIC’s evaluation of privacy legislation.

The Privacy Protection Working Group has an important responsibility as it sets standards through its model to build with durability in a way that both meets the needs of those consumers most concerned with making the requests governed by the model and that respects licensees’ need for a functional framework, workability, and exclusivity. Again, on behalf of its members, NAMIC appreciates that the Working Group now has scheduled – in-person and remote – open meetings to provide an opportunity for drafting regulators and interested parties to come together for focused discussions on the wording of the model. During these conversations, NAMIC plans to serve as a constructive resource in sharing possible approaches to (and possible wording suggestions for) developing a practical and stable legal framework for consumers’ privacy protection and options fitting for the insurance relationship and the consumers, licensees, and regulators that interact within in it.

NAMIC looks forward to working with the Privacy Protections Working Group in 2023. Thank you.



April 3, 2023

Via email: Lois Alexander ([lalexander@naic.org](mailto:lalexander@naic.org))  
NAIC Market Regulation Manager

Katie C. Johnson (VA), Chair  
Cynthia Amann (MO), Co-Vice Chair  
Chris Aufenthie (ND), Co-Vice Chair

Privacy Protections (H) Working Group  
National Association of Insurance Commissioners  
1100 Walnut Street  
Suite 1500  
Kansas City, MO 64106

**Re: Exposure Draft of National Association of Insurance Commissioners Consumer Privacy Protection Model Law (#674)**

Dear Chair Johnson, Vice Chairs Amann and Aufenthie, and Members of the Privacy Protections Working Group:

On behalf of the National Association of Professional Insurance Agents (PIA)<sup>1</sup>, thank you for the opportunity to provide comments on the National Association of Insurance Commissioners's (NAIC) draft model law.

We appreciate the Privacy Protections Working Group's attention to the issues presented by the existing NAIC models and the effects of evolving technologies on those models. The Working Group spent this past year engaged in conversation, first among its own regulatory members and then with some industry stakeholders, identifying the policy goals of its charge to use existing state insurance privacy protections to update, to the extent necessary, the NAIC's existing model laws governing the use of consumer data.

Ultimately, the Working Group concluded that the most logical way to achieve its goals would be to replace two existing NAIC models ([Model Act #670, the Insurance Information and Privacy Protection Model Act](#), hereinafter referred to as "Model #670," and [Model Regulation #672, the Privacy of Consumer Financial and Health Information Regulation](#), hereinafter referred to as "Model #672"), with a single new one. As a result, earlier this year, the Working Group

---

<sup>1</sup> PIA is a national trade association founded in 1931 whose members are insurance agents and agency owners in all 50 states, Puerto Rico, Guam, and the District of Columbia. PIA members are small business owners and insurance professionals serving insurance consumers in communities across America.



exposed the first draft of its new [Consumer Privacy Protection Model Law \(Model Law #674\)](#) (herein referred to as the “draft Model #674” or “the draft”) for comment by interested regulators and other interested stakeholders.

### **1. PIA shares the Working Group’s goal of protecting insurance consumer data.**

PIA appreciates the work that has gone into the exposure of this draft as well as the time the Working Group has already devoted to the subject over the past several months. We also appreciate the time allocated to consideration of the draft during the recent NAIC National Meeting in Louisville, and we look forward to continued collaboration with Working Group members and other interested parties during future open calls and the planned interim Working Group meeting.

We share the Working Group’s goals of ensuring that consumer data is protected; that they know how their data is being used; that they have the right to opt out of sharing their data, other than for insurance-related purposes; and that they are aware of that right and given the opportunity to exercise it. We recognize the value of giving consumers the power to limit the circumstances in which their data may be shared. We also recognize that data belonging to insurance consumers is particularly susceptible to exploitation because of the extent to which transmission of consumers’ personal information is required in the purchase of an insurance product.

Additionally, as noted in the [memo accompanying the exposure of draft MDL #674](#), the two existing NAIC models that would be superseded by this draft are decades old. In the time since the passage of each model, substantial technological advances have driven the evolution of every aspect of the insurance industry, including the work of independent insurance agents. Licensees will serve consumers better with updated guidance, and states will be better equipped to protect consumers and strengthen existing state insurance markets by giving state regulators the tools they need to protect both consumer data and the state-based insurance regulatory system.

As members of the Working Group may know, earlier this year, the 118<sup>th</sup> Congress turned its attention to the protection and privacy of consumer data, an issue that has arisen in Congress over the past several years. In late February, the House Financial Services Committee marked up [H.R. 1165, the Data Privacy Act](#), which Committee Chairman Patrick McHenry (R-NC) had identified as one of his top priorities for the year. H.R. 1165 passed out of Committee along a party-line vote but, as of the time of this writing, has not been considered by the full House.

Shortly thereafter, the House Committee on Energy and Commerce Subcommittee on Innovation, Data and Commerce held a hearing on the broader issue of privacy and data security across economic sectors.<sup>2</sup> Members of Congress are following this issue—and the NAIC’s consideration of it—closely. As in other areas of insurance law, the industry risks ever more

---

<sup>2</sup> This early activity in the 118<sup>th</sup> Congress’s Energy and Commerce (E&C) Committee is especially significant because the [American Data Privacy and Protection Act \(ADPPA\)](#) successfully passed out of the E&C Committee last year with bipartisan support. The ADPPA came close to becoming law near the end of 2022, when it was considered as a possible “rider” that might ultimately have been attached to different pieces of “must-pass” legislation. The ADPPA did not become law last year, and it is expected to be reintroduced in some form in the 118<sup>th</sup> Congress.

intrusive Congressional intervention, should the NAIC process not yield a model worthy of widespread support from state regulators, members of industry, and consumer groups, and, ultimately, worthy of adoption across the states. With that in mind, we ask the members of the Working Group to view our comments in the spirit with which we intend them: not to derail the drafting process but to improve its outcome.

PIA's concerns with the MDL #674 exposure draft are set forth below. Where applicable, our recommendations are reflected by tracked changes in the attached draft markup.

**2. As we understand the goals of the Working Group, they are inconsistently and insufficiently reflected in the draft.**

Following our March 31 conversation with Working Group Chair Katie Johnson (VA), we understand that the intent of the Working Group is ultimately for the model to permit licensees the unlimited<sup>3</sup> use and sharing of consumer data to the extent necessary to engage in insurance transactions.<sup>4</sup> The model is meant to limit the collection, processing, retention, or sharing of consumer data when such data is not being used in pursuit of insurance transactions.<sup>5</sup>

Working Group members seek to circumscribe the behavior of licensees who sell their clients' information without their clients' consent, without offering their clients an opportunity to "opt out" of having their data sold, or when they sell such data to businesses that are not engaged in the sale, solicitation, or negotiation of insurance, like the landscaping business described below in footnote 5.

However, the draft does not consistently reflect this distinction, and we hope the recommendations described herein and implemented in the attached markup, will assist Working Group members in ensuring that the model reflects their intent. Similarly, although the draft does not consistently reflect this understanding, members of the Working Group know that the role of independent insurance agents in such transactions is unique, particularly as compared with that of captive agents and insurance carriers.

---

<sup>3</sup> Such use and sharing of consumer data would remain subject to all existing applicable state and federal laws and regulations.

<sup>4</sup> Proper sharing of consumer data is intended to include the necessary sharing that occurs between independent insurance agents and their agency management systems (AMSs), through which agents communicate with the multitude of insurance carriers with which they have business relationships. Without AMSs, independent agents would be unable to scale their communications (requests for quotes, reports of claims, etc.) with their carrier partners competitively in the modern era.

<sup>5</sup> As an example, an independent insurance agent selling a homeowners' policy to a client is permitted to use the client data collected for the purpose of selling the homeowners' policy (and, for public policy reasons, should be encouraged) as a basis for speaking with that client about purchasing flood insurance, if the agent believes the client would benefit from flood insurance coverage (based on, for example, local floodplain management information, the location of the home in a flood-prone area, relevant FEMA maps, expertise in the area where the property is located, etc.).

On the other hand, that same independent insurance agent selling a homeowners' policy to a client would not, according to members of the working Group, be permitted to share that client data with an affiliated landscaping business in the hopes that the client will hire the landscaping business to provide the client with lawn care on their newly acquired property in the future. The former data usage is permitted, and the latter prohibited, because the former is in furtherance of an insurance transaction, while the latter is not.

We generally support the Working Group's goals as described above, but we are concerned that they are reflected inconsistently and inadequately in the draft. Through these comments and the attached markup, we will offer insight into the areas that insufficiently address the unique position of independent insurance agents or that conflict with the stated goals of the Working Group in ways that would be harmful to the independent agency system.

**3. The Purpose set forth in Article I, Section 1(A) does not appear to fully reflect the goals of the Working Group.**

To minimize the disconnect between our understanding of the Working Group's goals and the language in the draft, the attached markup includes the following suggested revisions to the Purpose provision.

**a. The Purpose does not adequately distinguish between insurance and noninsurance transactions.**

We found that no distinction was made between licensees' handling of consumer data for the purpose of engaging in the sale, solicitation, or negotiation of insurance and licensees' handling of consumer data for purposes unrelated to the business of insurance. We added language to establish that distinction at the beginning of the draft, so that vital context is made available to the reader immediately.

**b. The Purpose inaccurately suggests that consumer power over use of personal data may be unlimited.**

While PIA supports the right of consumers to grant or deny permission to insurance licensees regarding the use of their data, that right is not entirely unfettered. Consumers cannot, for example, purchase an auto insurance policy from an insurance agent without providing their drivers' license or Vehicle Identification Number (VIN), nor can they purchase a homeowners' insurance policy without providing the address of the property they wish to insure. Additionally, allowing consumers to choose which individual elements of their data may be collected, sold, or shared would place a costly administrative and financial burden on licensees and, depending on their size, could quickly drain them of human and financial resources.

For these reasons, we concluded that Article I, Section 1(A)(2), which would permit consumers to choose what personal information a licensee may "collect, process, retain, or share," is overly broad and could be unintentionally misleading. We hope that the more circumscribed language offered in the attached markup meets the needs of the Working Group and more accurately reflects the options available to consumers.

**c. The wording of Purpose Section 1(A)(5) is puzzling.**

We were perplexed by the wording of the provision purporting to offer a consumer the opportunity to access a licensee's version of their data so that the consumer may verify or dispute its accuracy. The spirit of this provision originated in Model #670, and we appreciate the

Working Group's notable efforts to achieve a comparatively streamlined version of the provision contained there.

However, the draft language leaves unclear whether a consumer must request access to their information from a licensee or whether the licensee is obligated to provide such access to all consumers regardless of whether they request it. Additionally, it refers both to "individual consumers" (plural) and then "the consumer" (singular), even though both refer to the same single consumer. The provision is also ambiguous about with whom this "access" resides, even though consumer access must necessarily be provided by the licensee whose record of the information is at issue.

We hope the revisions in the attached reflect our concerns with the draft Purpose language and the improvements we have described herein. To the extent that the attachment includes substantive changes to the Purpose section that are not discussed here, they are addressed elsewhere in these comments.

**4. The Drafting Note that precedes Article I, Section 2 could be clarified and moved further up in the draft.**

We understand that the Working Group intends for the current exposure draft, once finalized, to replace both Model #670 and Model #672. As such, the Drafting Note that precedes Article I, Section 2 seems unnecessarily opaque. A clearer rendition would be more useful if it appeared earlier in the draft and explicitly stated that this model is intended to replace Models #670 and #672. The first three sentences of the Drafting Note are serviceable as written, but they fail to state the obvious: that, following the finalization of Model #674, and subject to any requisite administrative NAIC proceedings, Models #670 and #672 will no longer be effective. That vital information is withheld, seemingly from the entire draft. Adding that information to the Drafting Note and moving it to the beginning of the draft would provide essential context to the reader at the point when such context is most needed.

Moreover, while Model #672 has been adopted by every state, Model #670 has not. As such, the part of the final sentence of the Drafting Note saying that this model "will supplant any [consumer privacy] notices required" by Model #670 or Model #672 is potentially confusing. States that have adopted only Model #672 or both models will presumably repeal and replace one or both in full, including the provisions governing consumer privacy notice requirements, in favor of the final version of the current draft. In that case, declaring that the consumer privacy notice requirements of both Models specifically have been supplanted is unnecessary and could needlessly confuse state lawmakers, regulators, licensees, and consumers, because they could infer incorrectly from it that other provisions of the Models remain in effect. The potential for confusion is exacerbated by the fact that the Drafting Note is placed at a point in the draft that does not specifically address consumer privacy notice requirements.

The wording of the Drafting Note also suggests that Models #670 and #672 themselves have the power to impose requirements on state licensees. In fact, state licensees are required to abide by the consumer privacy notice requirements promulgated in Models #670 and/or #672 because the models were adopted by states.

Likewise, the reference to the Gramm-Leach-Bliley Act (GLBA) at the end of the final sentence of the Drafting Note suggests that the GLBA, a federal law, directly imposed consumer notice requirements on state licensees. Rather, the GLBA included an instruction to states to adopt consumer privacy notice requirements. That instruction was the catalyst for the NAIC's promulgation of Model #672. That detail is elided in the final sentence of the existing Drafting Note but reflected in the revisions contained in the attached.

**5. For the draft to be workable, its requirements should be explicitly scalable.**

In recognition of the size and capacity variations among licensees, licensees' Model #674 obligations should be commensurate with their capacity to undertake such obligations. The NAIC's [Insurance Data Security Model Law, Model #668](#), acknowledged these variations and advised licensees to appropriately scale their Information Security Program and Risk Assessment and Management requirements such that they are commensurate with that licensee's size, scope, and complexity and the scope and complexity of its activities. However, even though the Model #674 draft liberally borrows from Model #668 elsewhere, the draft does not contain similar scalability language.

Licensees vary in size, scope, and complexity regardless of the role they play in the insurance industry, of course. However, independent insurance agencies *especially* vary enormously in size, number of employees, annual revenue, book of business value, and in the availability of nearly every imaginable resource. For that reason, PIA recommends adding a new Section 2, just before the draft's existing Section 2, setting forth a scalability provision using language similar to that used in Model #668.

If the Working Group accepts this addition, subsequent sections will require renumbering.

**6. Licensees' oversight obligations as to third parties should be set forth in more granular detail based on the nature of the third party, the nature of the licensee, and the nature of the activities they intend to undertake together.**

Article I, Section 2(A) of MDL #674 sets forth licensees' obligations with regard to the oversight of all third-party service providers and the agreements governing the relationships between licensees and their third-party service providers. Like the definition of the term "third-party service provider" itself, which we will further address below, these obligations do not distinguish among different types of third-party service providers; they demand strict adherence regardless of the types of licensees and third-party service providers at issue. In the preceding section, we addressed the issue of variations among licensees, and we have suggested a minor change to the beginning of Section 2(A) to reflect the scalability concern mentioned above.

**a. Licensees' oversight obligations as to third parties should distinguish between third parties engaged in the business of insurance or insurance-adjacent business, or those engaged in business activities unrelated to insurance.**

We now turn our attention to how differences among licensees should be considered in the context of third-party service providers, as well as variations among those third-party service providers themselves, and how the draft can adequately capture the possible combinations of licensees and third-party service providers and remain appropriately suited to all involved.

For example, our March 31 conversation with Chair Johnson suggested that the draft would benefit from establishing a more overt distinction between third-party service providers that are themselves engaged in the business of insurance or insurance-adjacent activity, and those whose primary business purpose is outside the realm of insurance.

Currently, the draft imposes the same obligations on all third-party service providers, whether the service they provide is related to insurance or not. However, third-party service providers outside the insurance industry are not otherwise subject to the requirements of the draft (or its predecessors, for that matter). Plus, the state insurance regulatory authorities ultimately responsible for enforcing these requirements have no authority over non-insurance-related third-party service providers. For these reasons, we have modified the language in the draft so that a licensee and a third-party service provider must enter into an agreement that conforms to the requirements of the draft when the agreement pertains to the business of insurance. We also modified the definition of "third-party service provider" to pertain only to third-party service providers that obtain or provide consumer data for purposes that are related to the business of insurance.

Moreover, we have also strengthened the language so that, where the third-party service provider involved in the business of insurance is subject to stricter standards than those contained in the draft, the draft standards serve as a floor rather than a ceiling. In other words, if a third-party service provider involved in the business of insurance is subject both to the draft standards and to more stringent standards, like those contained in the General Data Protection Regulation (GDPR), for instance, the third-party service provider must continue to comply with the relevant GDPR standards, assuming that they are more restrictive than the standards contained in the draft.

**b. Licensees cannot be made to negotiate contract terms with much larger and more powerful contract partners, particularly if those partners are not in the insurance industry.**

While these changes alleviate some of our concerns regarding the treatment of licensees in the context of third-party service providers, several concerns remain. In many relationships between independent insurance agents and third-party service providers, the independent agent has comparatively minimal negotiating power, irrespective of whether the third-party service provider is engaged in insurance-related business or not.

Because of the size and power disparity between many licensees (especially independent insurance agents) and the third-party service providers with whom they work, many licensees will face resistance to any demand that a third-party service provider execute a written agreement requiring its adherence to MDL #674, but the Act offers no alternative. It prohibits licensees from entering into any agreement or contract that allows any third-party service provider, irrespective of whether they are engaged in the business of insurance or not, to “collect, process, retain, or share” any consumer information in a prohibited manner.

Our concerns arise out of the frequency with which contracts of adhesion are utilized by large third-party service providers who are not engaged in the business of insurance and seek to exploit the size and power disparity between themselves and the small independent insurance agencies with whom they do business. This issue is most troubling when considered in the context of non-insurance-related businesses, because those engaged in the business of insurance or an adjacent insurance-related businesses often find it in their interest to comply with insurance-related standards, and they can expect to receive pressure from insurance business partners of all sizes if they delay doing so.

As an example of an insurance-related business for which compliance would be a priority even in the absence of small independent agencies, independent insurance agents rely heavily on agency management systems (AMSs) to communicate with the carriers with whom they partner. AMSs transmit consumer data gathered by the independent agent to their carrier partners and convey proprietary information, including policy quotes, marketing materials, and product design information, from the carrier to the agent.

As we understand it, the Working Group’s intent is to permit the largely unlimited exchange of consumer information among licensees in settings like those that exist within AMSs. Fortunately, because of their extensive connections to large insurance carriers, AMSs are likely already subject to standards similar to those contained in the draft; plus, if they were not already, they are subject to this draft’s standards by virtue of their existing relationship to carriers. Thus, while independent agents with small businesses often enter into “contracts of adhesion” out of necessity, their AMS contracts likely already comply with the draft. If they do not already, the AMS will likely make the change promptly, both to conform with applicable requirements, of course, but also because they will likely have received similar requests from other carriers and agents with whom they do business.

By contrast, the “contract of adhesion” issue persists among independent agents in their business arrangements with large, non-insurance-related companies. Corporate behemoths like Microsoft, Google, and Amazon will be reticent to change their existing data privacy practices to comply with laws that apply only to insurance licensees in certain states. Small-business licensees rarely have the luxury of negotiating the details of their relationships with relatively large third-party service providers. And when the primary business of those service providers is not insurance, compliance with NAIC models is not a given. Many licensees will be left with two unsavory options: they can be subjected to whatever consumer data privacy practice the third-party service provider typically uses, whether that practice meets the standards set forth in the draft of MDL #674, or they can altogether avoid any business relationship with the third-party service provider at issue—and probably entire categories of third-party service providers.

To create a distinction between third-party service providers engaged in the business of insurance or insurance-adjacent activities and third-party service providers engaged in non-insurance activities, we have provided recommended changes to the definitions of “third-party service provider” and “nonaffiliated third party” below.

**7. Some of the draft’s definitions are inconsistent with our understanding of the Working Group’s intent.**

**a. Article I, Section 3(B): “Additional permitted transactions”**

The definition of the term “additional permitted transactions” is both narrower and less clear than the Working Group may have intended. While it is possible that a licensee’s use of consumer data for a non-insurance-related purpose will result in a “transaction,” it is unclear whether the term “additional permitted transactions” is meant to refer only to transactions involving the consumer whose data is at issue or to refer to transactions that exclude the consumer but involve the licensee and/or the third party with whom the data is shared.

Regardless, we conclude that the licensee and any third-party recipients of the data are at least as likely to be engaged in “activities” as “transactions” unrelated to the business of insurance. Such activities could, but would not necessarily, result in transactions. We thus recast this term as “additional permitted activities” in its definition, and we attempted to make that change globally throughout the document, though we may not have succeeded.

We also conclude that Section 3(B)(1) is likely intended to refer to the marketing of non-insurance-related products or services and revised that provision accordingly. Similarly, we expect that the research activities identified in Section 3(B)(2) are unrelated to providing the consumer with insurance and have thus revised that portion as well.

**b. Article I, Section 3(C): “Adverse underwriting decision”**

We recognize that the refusal of a producer “to apply for insurance coverage with a specific insurer represented by the producer and that is requested by the consumer” is adapted from current Model Act #670, the *Insurance Information and Privacy Protection Model Act*.

However, we are concerned about the effect of Article I, Section 3(C)(1)(d) on independent agents’ freedom to manage their agencies as they see fit.

Agents adjust their strategies to meet the needs of their clients every day. If an agent does not apply for coverage with a specific carrier partner in accordance with a consumer’s request, they likely have a valid reason for that choice, and it should not be subject to evaluation by the consumer. Our concern about this provision is exacerbated by the draft’s broad definition of “consumer,” in which a consumer is defined as, among other things, a current or former applicant, policyholder, beneficiary, or claimant.

According to the draft, then, a producer will owe an explanation to a new prospective client if the producer does not apply for coverage with a specific insurer, where the producer represents that insurer and where the prospect requests such coverage be pursued. This requirement is overly



burdensome and will risk producers having to change their ordinary course of business to accommodate a prospect who may never become a client. We therefore recommend striking Article I, Section 3(C)(1)(d) in full and re-lettering the subparts that follow.

Section 3(C)(2) describes events that are *not* considered “adverse underwriting decisions,” but they require the consumer to be provided with a written reason(s) for the occurrence. The first two events are the issuance of a policy termination form “on a class or state-wide basis” [Section 3(C)(2)(a)] or a denial of coverage solely because such coverage is not available “on a class or state-wide basis” [Section 3(C)(2)(b)]. Because they are specific to class- or state-wide decisions, these two provisions will require information more readily available to the carrier than to the producer, making the carrier the best source of the requisite disclosure.

Likewise, the third of these are clearly the exclusive purview of the insurer, not the producer. There are no circumstances in which the responsibility for providing a consumer with an explanation of an “insurer-initiated” increase in premium should be assigned to a producer; producers should not be tasked with responding to these inquiries.

Additionally, while Section 3(C)(2)(c) explicitly states that consumers are entitled to explanations only upon request, Sections 3(C)(2)(a) and 3(C)(2)(b) are silent as to whether the consumer must initiate an inquiry to receive the information. We recommend that producers be relieved of the responsibility of responding to consumer requests arising from these provisions. We further recommend that the first two subparts also require a consumer request to initiate these disclosures. Finally, we recommend that insurers alone be responsible for providing them.

**c. Article I, Section 3(N): “De-identified”**

The definition of “de-identified” seems overly broad. It requires licensees to design and create business processes meant to prevent the accidental release of de-identified information, but it is far too expansive. It requires the protection of information that can “relate to” or “describe” a consumer; hair color can “describe” a consumer, and the town in which a consumer resides can “relate to” that consumer. In the attached, we offer revisions to narrow this definition to information that, if inadvertently disclosed, could be linked with a specific consumer, not a group of consumers that could number in the thousands.

**d. Article I, Section 3(T): “Insurance Support Organization”**

In Section 3(T)(1)(c), within the definition of “insurance support organization,” we offer revisions to the second mention of the word “transaction” to “activity” to enable it to conform with similar changes described in our discussion of the definition of “additional permitted transactions” above.

**e. Article I, Section 3(Z) (new definition): “Non-insurance-related third-party service provider”**

Below and in the attached, we offer a revised definition of “third-party service provider” that limits the definition to providers whose services relate to the business of insurance. That change

will exclude third-party service providers whose services are unrelated to the business of insurance, prompting the need for them to be defined elsewhere. In so doing, we recommend using the existing definition of third-party service provider as a basis while removing the reference to “insurance support organizations,” because they are necessarily associated with the business of insurance.

The definition set forth in the attached is located in alphabetical order within the “Definitions” section. If the Working Group accepts this addition, subsequent definitions will require relettering.

**f. Article I, Section 3(BB): “Personal information”**

We recognize that the definition of “personal information” is adapted from a combination of definitions included in current Models #670 and #672. However, in those models, the terms “relates to” and “describes” were limited to health care and financial information. Here, on the other hand, these terms encompass consumer information gathered in the process of engaging in any transaction, be it an insurance transaction or not. We recommend removing these descriptors because they are vague and could apply to so many characteristics that could not be easily linked with an individual consumer.

**g. Article I, Section 3(LL): “Share,” “shared,” or “sharing”**

Both before and after Section 3(LL), the phrase “additional permitted transactions” is used consistently throughout the draft. However, in Section 3(LL), “other permitted transactions” is used. We cannot be sure whether the Working Group’s intent is for this phrase to refer to “additional permitted transactions.” For that reason, we offer a revised term that we hope reflects both the Working Group’s preferred “additional” as well as our suggested change to “activities,” but we also hope to draw the Working Group’s attention to this question via our comment in the attachment.

We have some additional recommendations to the definition of “share” and its derivatives based on our understanding of the Working Group’s intent. First, we recommend the addition of language indicating that the sharing of consumer information would be “for the purpose of engaging in” additional permitted activities. Without this phrase, we are unable to discern the purpose of the original phrase “including other permitted transactions.”

We suggest striking the phrase “in which no valuable consideration is exchanged” at the end of the definition, because it is redundant with the portion that states, “whether or not for monetary or other valuable consideration.” The latter phrase covers both scenarios—involving the exchange of valuable consideration and scenarios where no valuable consideration is exchanged.

We also suggest adding “including the consumer” to the phrase “for the benefit of any party,” because we find it unclear whether “any party” is meant to refer only to those specifically mentioned in the definition, or any party at all. Bearing in mind the Working Group’s focus on the marketing of non-insurance-related products and services to insurance consumers, our recommendations seek to ensure that this definition reflects our understanding of that concern.

#### **h. Article I, Section 3(NN): “Third-party service provider”**

As drafted, the definition of “third-party service provider” does not distinguish between third-party service providers that are engaged in the business of insurance, like AMSs, and third-party service providers that are attempting to capitalize on the aggregation of consumer data for the purpose of marketing products and services that are unrelated to insurance. Based on our understanding of the Working Group’s priorities, we suggest adding “for the purpose of engaging in insurance-related business activities” to the definition, so that the term “third-party service provider” refers only to entities that obtain consumer information for insurance-related purposes, rather than all entities.

That change makes all “third-party service providers” inherently insurance-related and creates a need for a new definition of “non-insurance-related third-party service providers,” which we added as new Section 3(Z) and described above.

#### **8. Article II, Section 4(H) is overly restrictive and inconsistent with other provisions contained in the draft, and it would improperly prohibit independent agents from selling insurance policies to consumers.**

As drafted, Article II, Section 4(H) prohibits licensees from selling or sharing consumer information in exchange for any consideration. However, elsewhere in the draft, licensees are granted express permission to share consumer information in furtherance of the solicitation, sale, and negotiation of insurance.

Inevitably, such activities can result in the exchange of consideration; if an independent agent is successful, they will receive first information and ultimately payment from consumers, who will, in exchange, receive insurance policies. Similarly, the independent agent will have exchanged that consumer information with an AMS and at least one carrier, which will, if they are successful, also result in the exchange of consideration. At a minimum, this section requires substantial refinement. However, the ostensible goal of this provision, to prevent the outright sale of consumer information by licensees, is achieved elsewhere in the model. As such, we recommend its deletion.

#### **9. Remove the draft’s optional private right of action.**

The inclusion of an optional private right of action threatens the future of the independent agency system, so we were pleased to learn that the Working Group has decided to omit it going forward. In accordance with the expressed desire of the Working Group, we have stricken Article VII, Section 28 from the attached draft.

#### **10. If finalized as written, the model will challenge independent agents’ ability to conduct their business operations.**

Upon our initial review of the draft, we had concerns about the limitations it appeared to place on independent agents to provide information to consumers that may assist them in filling insurance coverage gaps they may not otherwise have realized exist. We feared that the draft language

would prohibit an agent who sold homeowners' insurance, for example, from recommending flood insurance in an area prone to flooding.

However, since our initial review, we have come to understand that the Working Group does not intend to prohibit those activities. We had concerns about agents' ability to compete for the business of former clients because the draft appeared to prohibit agents from retaining even the most basic contact information of prior clients. We realize, however, that state and federal document retention requirements will continue to ensure that agents are able to retain some basic information about their former clients and enable them to compete for those clients' business.

Naturally, agents also face the risk of being involved in litigation, be it between a client and an insurance carrier over whether coverage exists, between a client and a carrier over the amount of damages paid on a covered loss, between a client and an agent over an errors & omissions claim, or any other dispute that advances to litigation. The retention of relevant documents is vital to any possible reconstruction of the disputed event in litigation, irrespective of the events giving rise to the suit. We also had concerns that the draft inadvertently requires licensees to discard data and documentation that would otherwise be retained for litigation purposes. Again, though, state and federal document retention requirements will ensure that paperwork associated with claims and potential litigation will be appropriately retained.

## **11. Conclusion**

Our comments here are far from exhaustive; we know that the Working Group expects additional feedback from us, and we have additional input we plan to provide. We look forward to a productive conversation with Working Group members on a call scheduled for later this month. At that time, we hope to be able to provide additional insights into our members' current data-sharing and consumer opt-out practices, among other issues. We appreciate the Working Group's flexibility and recognition of concerns that are specific to the independent agent community. As always, we appreciate the opportunity to provide the independent agent perspective.

Please contact me at [lpachman@pianational.org](mailto:lpachman@pianational.org) or (202) 431-1414 with any questions or concerns. Thank you for your time and consideration.

Sincerely,



Lauren G. Pachman  
Counsel and Director of Regulatory Affairs  
National Association of Professional Insurance Agents

Enclosure

**Insurance Consumer Privacy Protection Model Law #674**

**2023 Privacy Protections Working Group**

**Contents**

ARTICLE 1. GENERAL PROVISIONS..... 3  
Section 1. Purpose and Scope ..... 3  
Section 2. Oversight of Third-Party Service Provider Arrangements ..... 4  
Section 3. Definitions ..... 5  
ARTICLE II. OBLIGATIONS HANDLING CONSUMER'S PERSONAL INFORMATION..... 16  
Section 4. Data Minimization and Sharing Limitations ..... 16  
Section 5. Retention and Deletion of Consumers' Information..... 19  
ARTICLE III. NOTICES AND AUTHORIZATIONS..... 21  
Section 6. Initial and Annual Notice of Consumer Information Practices..... 21  
Section 7. Content of Consumer Information Practices Notices ..... 22  
Section 8. Delivery of Notices Required by This Act..... 25  
Section 9. Consumers' Consent- How Obtained ..... 26  
Section 10. Content of Authorizations ..... 28  
ARTICLE IV. CONSUMERS' RIGHTS ..... 30  
Section 11. Access to Personal Information..... 30  
Section 12. Correction or Amendment of Personal Information..... 31  
Section 13. Nondiscrimination and Nonretaliation ..... 32  
ARTICLE V. ADVERSE UNDERWRITING DECISIONS; OTHER TRANSACTIONS [OPTIONAL] ... 34  
Section 14. Adverse Underwriting Decisions ..... 34  
Section 15. Information Concerning Previous Adverse Underwriting-Decisions..... 35  
Section 16. Previous Adverse Underwriting-Decisions ..... 35  
ARTICLE VI. ADDITIONAL PROVISIONS ..... 36  
Section 17. Pretext Interviews [OPTIONAL] ..... 36  
Section 18. Investigative Consumer Reports [OPTIONAL] ..... 36  
Section 19. Compliance with HIPAA and HITECH ..... 37  
ARTICLE VII. GENERAL PROVISIONS..... 38  
Section 20. Power of Commissioner ..... 38  
Section 21. Confidentiality ..... 38  
Section 22. Record Retention ..... 39  
Section 23. Hearings, Records, and Service of Process ..... 39  
Section 24. Service of Process -Third-Party Service Providers..... 40  
Section 25. Cease and Desist Orders and Reports..... 41

**Insurance Consumer Privacy Protection Model Law #674**

**2023 Privacy Protections Working Group**

Section 26. Penalties..... 41  
Section 27. Judicial Review of Orders and Reports ..... 42  
Section 28. Individual Remedies..... 43  
Section 29. Immunity..... 44  
Section 30. Obtaining Information Under False Pretenses ..... 44  
Section 31. Severability..... 44  
Section 32. Conflict with Other Laws ..... 44  
Section 33. Rules and Regulations ..... 44  
Section 34. Effective Date ..... 45

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

**Drafting Note:** This model is intended to replace NAIC Model Law #670 and NAIC Model Regulation #672; for that reason, it includes the protections for consumers that are currently provided by Models #670 and #672 and adds additional protections that reflect the business practices in the insurance industry today. The business of insurance is more global than it was 30-40 years ago. This model law reflects those realities and addresses the need for additional consumer protections. This model requires notices to consumers for various privacy concerns and will supplant any notice requirements imposed by state authorities in accordance with Model #670, Model #672 and, via Model #672, the Gramm-Leach Bliley Act.

Commented [KJ1]: Based on Model 670

Commented [LP1]: This is a revised version of the Drafting Note that was originally located before Section 2.

## ARTICLE 1. GENERAL PROVISIONS

### Section 1. Purpose and Scope

- A. **Purpose:** This Act establishes (i) standards for the collection, processing, retaining, or sharing of consumers' personal information ~~for the purposes of enabling licensees to engage in the sale, solicitation, or negotiation of insurance and enabling licensees to engage in non-insurance-related activities, by licensees~~ to maintain a balance between the need ~~for information by of~~ those in the business of insurance ~~to collect, process, retain, and share information~~ and consumers' need for fairness and protection in the use of ~~consumers' their~~ personal information; (ii) standards for additional permitted ~~transactions—activities~~ involving ~~the collection, processing, retaining, or sharing of~~ consumers' personal information; and (iii) standards applicable to licensees for ~~providing~~ notice to consumers of the collection, processing, retention, or sharing of ~~consumers' their~~ personal information. These standards address the need to:
- (1) Limit the collection, processing, retention, or sharing of consumers' personal information to purposes required in connection with insurance transactions and additional permitted ~~activities~~ transactions;
  - (2) Enable consumers to ~~determine consent to the collection, processing, retention, or sharing of what their personal information by a licensee by requiring the licensee to provide consumers with the opportunity to opt into or out of additional permitted activities—~~is collected, processed, retained, or shared;
  - (3) Enable consumers to know the sources from whom consumers' personal information is collected and with whom such information is shared;
  - (4) Enable consumers to understand why and for generally how long personal information is retained;
  - (5) ~~Upon request, a~~Allow ~~an individual consumers-~~ to access ~~a licensee's rendition of that consumer's personal information—relating to the consumer requesting access, so that said consumer to—may~~ verify or dispute the accuracy of the information ~~held by the licensee~~; and
  - (6) Allow consumers to obtain the reasons for adverse underwriting transactions.
- B. **Scope:** The obligations imposed by this Act shall apply to licensees and third-party service providers, on or after the effective date of this Act:
- (1) ~~Who c~~Collect, process, retain, or share consumers' personal information in connection with insurance transactions;
  - (2) ~~Who e~~Engage in insurance transactions with consumers; or
  - (3) ~~Who e-~~Engage in additional permitted ~~transactions—activities~~ involving consumers' personal information.
- C. **Protections:** The rights granted by this Act shall extend to consumers:
- (1) Who are the subject of information collected, processed, retained, or shared in connection with insurance transactions;
  - (2) Who engage in or seek to engage in insurance transactions;

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (3) Who have engaged in the past in insurance transactions with any licensee or third-party service provider; or
- (4) Whose personal information is used in additional permitted ~~transactions~~activities by licensees and third-party service providers.

**Drafting Note:** This model is intended to include the protections for consumers that are provided by NAIC Model Law #670 and NAIC Model Regulation #672 and adds additional protections that reflect the business practices in the insurance industry today. The business of insurance is more global than it was 30-40 years ago. This model law reflects those realities and addresses the need for additional protections for consumers. This model requires notices to consumers for various privacy concerns and will supplant any notices required under Model #670, Model #672 and Gramm-Leach-Bliley.]

### Section 2. Variations in Licensee Size and Complexity

A licensee shall discharge the obligations set forth herein in a manner commensurate with the licensee's size and complexity, the nature and scope of the licensee's activities, including its use of third-party service providers, nonaffiliated third parties, and insurance support organizations; the extent to which it engages in additional permitted activities; and the sensitivity of the nonpublic information it collects, processes, retains, and shares.

Commented [KJ2]: Language taken from Model 668 (IDSA)

### Section 2. Oversight of Third-Party Service Provider Arrangements

- A. To the extent feasible, a licensee shall exercise due diligence in selecting its third-party service providers.  
No licensee shall (i) engage a third-party service provider to collect, process, or retain, or share any consumer's personal information, or (ii) share any consumer's personal information with any third-party service provider for any purpose related to the business of insurance unless there is a written agreement between the licensee and third-party service provider that requires the third-party service provider to abide at least by the provisions of this Act, if not stricter provisions imposed by another authority, and the licensee's own practices in the collection, processing, retention, or sharing of any consumer's personal information.
- B. A licensee shall require all the licensee's third-party service providers engaged in businesses that are related to the business of insurance to implement appropriate measures to comply with the provisions of this Act in relation to consumers' personal information that is (i) collected, processed, or retained by or (ii) shared with or otherwise made available to the third-party service providers in connection with (i) any insurance transactions of the licensee or (ii) any additional permitted ~~transactions~~activities.
- C. No agreement or contract between a licensee and a third-party service provider shall permit the third-party service provider to collect, process, retain, or share any consumer's personal information in any manner:
  - (1) Not permitted by this Act; and
  - (2) Not consistent with the licensee's own privacy practices.
- D. An agreement related to the business of insurance between a licensee and third-party service provider shall require that no third-party service provider shall further share or process a consumer's personal information other than as specified in the agreement(s) with the licensee.

Commented [LP2]: This drafting note has been moved to the beginning of the document.



## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

#### Section 3. Definitions

As used in this Act:

A. "Address of record" means:

- (1) A consumer's last known USPS mailing address shown in the licensee's records; or
- (2) A consumer's last known email address as shown in the licensee's records, if the consumer has consented under [refer to the state's UETA statute] to conduct business electronically.
- (3) An address of record is deemed invalid if

(a) ~~USPS mail sent to that address by the licensee has been returned as undeliverable and if subsequent attempts by the licensee to obtain a current valid address for the consumer have been unsuccessful; or~~

Commented [KJ3]: The language in this subdivision was taken from Model 672.

(b) The consumer's email address in the licensee's records is returned as "not-deliverable" and subsequent attempts by the licensee to obtain a current valid email address for the consumer have been unsuccessful.

B. "Additional permitted ~~transactions~~activities" means collecting, processing, retaining, or sharing a consumer's personal information, with the consumer's consent, for:

- (1) ~~The purpose of marketing purposes~~non-insurance-related products or services; or
- (2) Research activities not related to ~~the provision of insurance to the consumer whose information is being collected, processed, retained, or shared, or for rating,~~ or risk management purposes for or on behalf of the licensee.

Commented [KJ4]: By limiting AUDs in this manner, we provide consistency with current state law (for those states that adopted Model 670 and consistency with FCRA).

C. Adverse underwriting decision means:

- (1) Any of the following actions with respect to insurance transactions involving primarily personal, family, or household use:
  - (a) A denial, in whole or in part, of insurance coverage requested by a consumer;
  - (b) A termination of insurance coverage for reasons other than nonpayment of premium;
  - (c) A rescission of the insurance policy;
  - (d) ~~Failure of a producer to apply for insurance coverage with a specific insurer represented by the producer and that is requested by a consumer;~~
  - (e) In the case of a property or casualty insurance coverage:

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (i) Placement by an insurer or producer of a risk with a residual market mechanism, non-admitted insurer, or an insurer that specializes in substandard risks;
  - (ii) The charging of a higher rate based on information which differs from that which the consumer furnished; or
  - (f) In the case of a life, health, or disability insurance coverage, an offer to insure at higher than standard rates.
- (2) Notwithstanding subsection C 1, the following insurance transactions shall not be considered adverse underwriting decisions but, if requested by a consumer, the insurer ~~or producer~~ responsible for the occurrence shall provide the consumer with the specific reason or reasons for the occurrence in writing:
- (a) The termination of an individual policy form on a class or state-wide basis;
  - (b) A denial of insurance coverage solely because such coverage is not available on a class- or state-wide basis; or
  - (c) ~~If requested by a consumer,~~ any other insurer-initiated increase in premium on an insurance product purchased by a consumer.

**Drafting Note:** The use of the term "substandard" in Section ~~2CB(4)(e)(i)~~ is intended to apply to those insurers whose rates and market orientation are directed at risks other than preferred or standard risks. To facilitate compliance with this Act, Commissioners should consider developing a list of insurers operating in their state which specialize in substandard risks and make it known to insurers and producers.

- D. "Affiliate" or "affiliated" means a person that directly, or indirectly through one or more intermediaries, controls, is controlled by, or is under common control with another person.
- E. "Biometric information" means an individual's physiological, biological, or behavioral characteristics that can be used, singly or in combination with each other or with other identifying information, to establish a consumer's identity. Biometric information includes deoxyribonucleic acid (DNA), imagery of the iris, retina, fingerprint, face, hand, palm, ear, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.
- F. "Clear and conspicuous notice" means a notice that is reasonably understandable and designed to call attention to the nature and significance of its contents.
- G. "Collect" or "collecting" means buying, renting, gathering, obtaining, receiving, or accessing any consumers' personal information by any means.

**Commented [KJ5]:** Language from Model 672 in part.

**Commented [KJ6]:** Model 672 definition only applies to identified data: to obtain information that the licensee organizes or can retrieve by the name of an individual or by identifying number, symbol or other identifying particular assigned to the individual, irrespective of the source of the underlying information

January 31, 2023

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- H. "Commissioner" means [insert the appropriate title and statutory reference for the principal insurance regulatory official of the state].
- I. **Consumer** means an individual and the individual's legal representative, including a current or former (i) applicant, (ii) policyholder, (iii) insured, (iv) beneficiary, (v) participant, (vi) annuitant, (vii) claimant, or (viii) certificate holder who is a resident of this state and whose personal information is used, may be used, or has been used in connection with an insurance transaction. An individual that is a mortgagor of a mortgage covered under a mortgage insurance policy is a consumer. A consumer shall be considered a resident of this state if the consumer's last known mailing address, as shown in the records of the licensee, is in this state unless the last known address of record is deemed invalid.
- J. "Consumer report" means a written, oral, or other communication of information bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used in connection with an insurance transaction.
- K. "Consumer reporting agency" means a person who:
- (1) Regularly engages, in whole or in part, in the practice of assembling or preparing consumer reports for a monetary fee;
  - (2) Obtains information primarily from sources other than insurers; and
  - (3) Furnishes consumer reports to other persons.
- L. **Control** means:
- (1) Ownership, control, or power to vote twenty-five percent (25%) or more of the outstanding shares of any class of voting security of the company, directly or indirectly, or acting through one or more other persons;
  - (2) Control in any manner over the election of a majority of the directors, trustees or general partners (or individuals exercising similar functions) of the company; or
  - (3) The power to exercise, directly or indirectly, a controlling influence over the management or policies of the company, as the commissioner determines.
- M. "Delete" and "deleted" means to remove or destroy information such that it is not maintained in human or machine-readable form and cannot be retrieved or utilized in such form;
- N. **De-identified information** means information that alone cannot reasonably identify, ~~relate to, describe,~~ be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a licensee that uses de-identified information:

Commented [KJ7]: This definition is similar to that in Model 672.

Commented [KJ8]: Definition from Model 672

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (1) Has implemented technical safeguards designed to prohibit re-identification of the consumer to whom the information may pertain.
- (2) Has implemented reasonable business policies that specifically prohibit re-identification of the information.
- (3) Has implemented business processes designed to prevent inadvertent release of de-identified information.
- (4) Makes no attempt to re-identify the information.

O. "Health care" means:

Commented [KJ9]: Taken from Model 672

- (1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care, services, procedures, tests, or counseling that:
  - (a) Relates to the physical, mental, or behavioral condition of an individual; or
  - (b) Affects the structure or function of the human body or any part of the human body, including the banking of blood, sperm, organs, or any other tissue; or
- (2) Prescribing, dispensing, or furnishing drugs or biologicals, or medical devices, or health care equipment and supplies to an individual.

P. "Health care provider" means a health care practitioner licensed, accredited, or certified to perform specified health care consistent with state law, or any health care facility.

Commented [KJ10]: This definition comes from Model 672

Q. "Health information" means any consumer information or data except age or gender, created by or derived from a health care provider or the consumer that relates to:

Commented [KJ11]: This definition comes from Model 672

- (1) The past, present, or future (i) physical, (ii) mental, or (iii) behavioral health, or condition of an individual;
- (2) The genetic information of an individual;
- (3) The provision of health care to an individual; or
- (4) Payment for the provision of health care to an individual.

Commented [KJ12]: WG added this update to the definition

R. "Individual" means a natural person;

S. "Institutional source" means any person or governmental entity that provides information about a consumer to a licensee other than:

Commented [KJ13]: Model 670

- (1) A producer;
- (2) A consumer who is the subject of the information; or

**Insurance Consumer Privacy Protection Model Law #674**

**2023 Privacy Protections Working Group**

(3) An individual acting in a personal capacity rather than in a business or professional capacity.

T. "Insurance support organization" means:

Commented [KJ14]: Model 670

(1) Any person who regularly engages in the collection, processing, retention, or sharing of consumers' information for the primary purpose of providing insurers or producers information in connection with insurance transactions, including:

(a) The furnishing of consumer reports or investigative consumer reports to licensees or other insurance support organizations for use in connection with insurance transactions,

(b) The collection of personal information from licensees or other insurance support organizations to detect or prevent fraud, material misrepresentation, or material nondisclosure in connection with insurance transactions.

(c) The collection of any personal information in connection with an insurance transaction that may have application in an activity transactions ~~in~~ other than an insurance transaction.

(2) Notwithstanding Subdivision (1) of this subsection, producers, government institutions, insurers, health care providers shall not be considered "insurance support organizations" for purposes of this Act.

U. "Insurance transaction" means any transaction or service by or on behalf of a licensee involving:

Commented [KJ15]: Model 672 uses "Insurance product or service" means any product or service that is offered by a licensee pursuant to the insurance laws of this state.

(2) Insurance service includes a licensee's evaluation, brokerage or distribution of information that the licensee collects in connection with a request or an application from a consumer for a insurance product or service.

(1) The determination of a consumer's eligibility for or the amount of insurance coverage, rate, benefit, payment, or claim settlement;

(2) The servicing of an insurance application, policy, contract, or certificate, or any other insurance product;

(3) Provision of "value-added services or benefits" in connection with an insurance transaction;

(4) Any mathematical-based decision that involves a consumer's personal information; or

(5) Any actuarial or research studies for rating or risk management purposes conducted by or for the benefit of the licensee using consumers' personal information.

V. "Insurer" means

(1) Any person or entity required to be licensed by the commissioner to assume risk, or otherwise authorized under the laws of the state to assume risk,

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

including any corporation, association, partnership, nonprofit hospital, medical or health care service organization, health maintenance organization, reciprocal exchange, inter insurer, Lloyd's insurer, fraternal benefit society, or multiple-employer welfare arrangement;

- (2) A self-funded plan subject to state regulation.
- (3) A preferred provider organization administrator.
- (4) "Insurer" does not include producers, insurance support organizations, foreign-domiciled risk retention groups, or foreign-domiciled reinsurers.

**Drafting Note:** If the state regulates third party administrators who operate on behalf of insurers, the state may wish to add them to this list.

W. "Investigative consumer report" means a consumer report or portion of a consumer report in which information about an individual's character, general reputation, personal characteristics, or mode of living is obtained through personal interviews with the individual's neighbors, friends, associates, acquaintances, or others who may have knowledge concerning such items of information.

Commented [KJ16]: Definition from Model 670

X. "Licensee" means 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. "Licensee" shall also include an unauthorized insurer that accepts business placed through a licensed excess lines broker in this state, but only in regard to the excess lines placements placed pursuant to Section [insert section] of the state's laws.

Commented [KJ17]: This definition was taken from Model 668 but is very similar to the definition in Model 672

Y. "Nonaffiliated third party" means:

Commented [KJ18]: Model 672

- (1) Any person except:
  - (a) An affiliate of a licensee; or
  - (b) A person employed jointly by a licensee and any company that is not an affiliate of the licensee; however, a nonaffiliated third party includes the other company that jointly employs the person.
- (2) Nonaffiliated third party includes any person that is an affiliate solely by virtue of the direct or indirect ownership or control of the person by the licensee or its affiliate in conducting merchant banking or investment banking activities of the type described in Section 4(k)(4)(H) or insurance company investment activities of the type described in Section 4(k)(4)(I) of the federal Bank Holding Company Act (12 U.S.C. 1843(k)(4)(H) and (I)).

**Insurance Consumer Privacy Protection Model Law #674**

**2023 Privacy Protections Working Group**

Z. ~~"Non-insurance-related third party service provider" means any person that, for the purpose of engaging in activities unrelated to the business of insurance, obtains consumers' personal information from a licensee or provides consumers' personal information to a licensee or that:~~

Formatted: Font: (Default) Arial, 8 pt

~~(1) (a) Has access to consumers' personal information through the person's provision of: (i) any services to or on behalf of a licensee; (ii) electronic applications for use by the licensee's consumers; or (iii) any other products to or on behalf of the licensee in connection with insurance transactions; or (iv) the provision of services in connection with additional permitted activities; and~~

~~(b) Is any person not otherwise defined as a licensee; or~~

~~(2) Is a vendor of personal health records.~~

Formatted: Font: (Default) Arial, 8 pt

Z. ~~"Nonpublic Information" means information that is not publicly available information and is:~~

Commented [KJ19]: From Model 672

Any information concerning a consumer which because of name, number, personal mark, or other identifier can be used to identify such consumer, in combination with any one or more of the following data elements:

- (1) Social Security number,
- (2) Driver's license number or non-driver identification card number,
- (3) Account number, credit or debit card number,
- (4) Any security code, access code or password that would permit access to a consumer's financial account, or
- (5) Biometric information;

AA. "Person" means any individual, corporation, association, partnership, or other legal entity.

BB. "Personal information" means:

(1) Any individually identifiable information that identifies, ~~relates to, describes, is~~ reasonably capable of being associated with, or could reasonably be linked to a consumer that is:

Commented [KJ20]: From Model 670

- (a) Gathered in connection with an insurance transaction;
- (b) Gathered in connection with any other permitted transaction;

(2) Any of the following:

~~(a) Account balance information and payment history;~~

Commented [KJ21]: The information in F(1) (b)-(g) was taken directly from Model 672

- (b) The fact that an individual is or has been one of the licensee's customers or has obtained an insurance product or service from the licensee;
- (c) Any information about the licensee's consumer if it is disclosed in a manner that indicates that the individual is or has been the licensee's consumer, unless such disclosure is required by federal or state law for reporting purposes;
- (d) Any information that a consumer provides to a licensee or that the licensee or its agent otherwise obtains in connection with collecting on a loan or servicing a loan;
- (e) Any information the licensee collects through an information-collecting device from a web server, such as internet cookies;
- (f) Information from a consumer report;

**Insurance Consumer Privacy Protection Model Law #674**

**2023 Privacy Protections Working Group**

(g) Information that would enable judgments, directly or indirectly, to be made about a consumer's character, habits, avocations, finances, occupation, general reputation, credit, health, or any other personal characteristics; or

Commented [KJ22]: The provision in F.(1)(h) was taken from Model 670

- (3) "Nonpublic information";
- (4) "Publicly available information;"
- (5) "Sensitive personal information";
- (6) "Health information;" or
- (7) Consumers' demographic data, in any form or medium that can reasonably be used to identify an individual.
- (8) "Personal information" includes collections or sets of individually identifiable information pertaining to more than one consumer.
- (9) "Personal information" does not include "de-identified information."

CC. "Pretext interview" means an attempt to obtain information about an individual, where an interviewer does one or more of the following:

Commented [KJ23]: Model 670

- (1) Pretends to be someone the interviewer is not;
- (2) Pretends to represent a person the interviewer is not in fact representing;
- (3) Misrepresents the true purpose of the interview; or
- (4) Refuses to provide identification upon request.

DD. "Precise geolocation" means any data that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet.

EE. "Process" or "processing" mean: any operation or set of operations performed by a licensee, whether by manual or automated means, on the personal information of any consumer, including the collection, use, sharing, storage, disclosure, analysis, deletion, retention, or modification of data or personal information.

FF. "Privileged information" means any personal information that:

Commented [KJ24]: Model 670

- (1) Relates to a claim for insurance benefits or a civil or criminal proceeding involving a consumer; and
- (2) Is collected in connection with or in reasonable anticipation of a claim for insurance benefits or civil or criminal proceeding involving a consumer;

**Drafting Note:** The phrase "in reasonable anticipation of a claim" contemplates that the insurer has actual knowledge of a loss but has not received formal notice of the claim.



## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

GG. "Producer" means [refer here to every appropriate statutory category of producer, including brokers, required to be licensed to do business in the state].

**Drafting Note:** This is necessary because many states have various terms for producers, or for producers of certain types of insurers.]

HH. "Publicly available" means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from:

**Commented [KJ25]:** This definition comes from the IDSA (Model 668) and Model 672

- (1) Federal, state, or local government records;
- (2) Widely distributed media; or
- (3) Disclosures to the general public that are required to be made by federal, state or local law.

**Drafting Note:** Examples of "a reasonable basis" are: (1) A licensee has a reasonable basis to believe that mortgage information is lawfully made available to the general public if the licensee has determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded or (2) A licensee has a reasonable basis to believe that an individual's telephone number is lawfully made available to the general public if the licensee has located the telephone number online or the consumer has informed you that the telephone number is not unlisted.

**Commented [KJ26]:** Examples take from Modell 672

II. "Residual market mechanism" means an association, organization or other entity defined or described in Sections(s) [insert those sections of the state insurance code authorizing the establishment of a FAIR Plan, assigned risk plan, reinsurance facility, joint underwriting association, etc.]

**Commented [KJ27]:** Model 670 language

**Drafting Note:** Those states having a reinsurance facility may want to exclude it from this definition if the state's policy is not to disclose to insureds the fact that they have been reinsured in the facility.

JJ. "Retain" "retention" or "retaining" means storing or archiving personal information that is in the continuous possession, use, or control of licensee or a third-party service provider.

KK. "Sensitive personal information" means information that reveals (i) a consumer's social security, driver's license, state identification card, or passport number; (ii) a consumer's account log-in or financial account, debit card, or credit card numbers in combination with any required security or access code, password, or credentials allowing access to an account; (iii) a consumer's precise geolocations; (iv) a consumer's racial or ethnic origin, religious, or philosophical beliefs; (v) union membership; (vi) the contents of a consumer's personal mail, personal email, and personal text messages unless the person in possession is the intended recipient of the communication; (vii) a consumer's genetic data; (viii) a consumer's sex life or sexual orientation; (ix) a consumer's citizenship or immigration status; (x) a consumer's health information; or (xi) a consumer's biometric information.

**Drafting Note:** Those states that have enacted a consumer data protection act may want to amend this definition to match that of the state's law.

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

LL. "Share," "shared," or "sharing" means (i) disclosing, (ii) disseminating, (iii) making available, (iv) releasing, (v) renting, (vi) transferring, (vii) selling, or (viii) otherwise communicating by any means, a consumer's personal information (i) by a licensee to an insurance support organization or (ii) by a licensee or insurance support organization to a third-party service provider, whether or not for monetary or other valuable consideration, for the purpose of engaging in including other additional permitted ~~transactions~~ activities ~~between~~ involving a licensee and an insurance support organization or involving a licensee or insurance support organization and a third party service provider for the benefit of any party, including the consumer in which no valuable consideration is exchanged.

Commented [KJ28]: Model 670

Commented [LP3]: Should this be "additional" to be consistent with the rest of the draft? Assuming it is, I also changed "transactions" to "activities" to make that consistent as well.

MM. "Termination of insurance coverage" or "termination of an insurance policy" means either a cancellation or nonrenewal of an insurance policy, in whole or in part, for any reason other than failing to pay a premium as required by the policy.

Commented [KJ29]: From Model 668 but modified for this model

NN. "Third-party service provider" means any person that, for the purpose of engaging in insurance-related business activities, obtains consumers' personal information from a licensee or provides consumers' personal information to a licensee or that:

- (1) (a) Has access to consumers' personal information through the person's provision of: (i) any services to or on behalf of a licensee; (ii) electronic applications for use by the licensee's consumers; or (iii) any other products to or on behalf of the licensee in connection with insurance transactions; or (iv) the provision of services in connection with additional permitted ~~transactions~~ activities; and
- (b) Is either (i) an insurance support organization; or (ii) any person not otherwise defined as a licensee; or
- (2) Is a vendor of personal health records.

Commented [KJ30]: Definition from Model 670

OO. "Unauthorized insurer" means an insurer that has not been granted a certificate of authority by the Commissioner to transact the business of insurance in this state.

Drafting Note: Each state must make sure this definition is consistent with its surplus lines laws.

PP. "Value-added service or benefit" means a product or service that:

Commented [KJ31]: This definition was taken primarily from Model 880 (rebating)

- (1) Relates to insurance coverage applied for or purchased by a consumer; and
- (2) Is primarily designed to satisfy one or more of the following:
  - (a) Provide loss mitigation or loss control;
  - (b) Reduce claim costs or claim settlement costs;
  - (c) Provide education about liability risks or risk of loss to persons or property;

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (d) Monitor or assess risk, identify sources of risk, or develop strategies for eliminating or reducing risk;
- (e) Enhance the health of the consumer, including care coordination;
- (f) Enhance financial wellness of the consumer through education or financial planning services;
- (g) Provide post-loss services;
- (h) Incentivize behavioral changes to improve the health or reduce the risk of death or disability of a customer (defined for purposes of this subsection as policyholder, potential policyholder, certificate holder, potential certificate holder, insured, potential insured or applicant); or
- (i) Assist in the administration of employee or retiree benefit insurance coverage.

**Drafting Note:** Examples of "value-added services and benefits" are services or benefits related to (i) health and wellness, (ii) telematic monitoring, or (iii) property replacement services.

QQ. "Written consent" means any method of capturing a consumer's consent that is capable of being recorded or maintained for as long as the licensee has a business relationship with a consumer; or the licensee or service provider is required to maintain the information as provided in this Act.

**Insurance Consumer Privacy Protection Model Law #674**

**2023 Privacy Protections Working Group**

**ARTICLE II. OBLIGATIONS HANDLING CONSUMER'S PERSONAL INFORMATION**

**Section 4. Data Minimization and Sharing Limitations**

- A. No licensee shall collect, process, retain, or share a consumer's personal information unless:
- (1) The collection, processing, retention, or sharing is in connection with an insurance transaction as defined in this Act;
  - (2) The licensee provides the applicable notices required by this Act;
  - (3) The collection, processing, retention, or sharing of the consumer's personal information is consistent with and complies with the most recent notice provided to the consumer by the licensee;
  - (4) The collection, processing, retention, or sharing of the consumer's personal information is reasonably necessary and proportionate to achieve the purposes related to the requested insurance transaction or additional permitted ~~transactions-activities~~ and not further processed, retained, or shared in a manner that is incompatible with those purposes; and
  - (5) The licensee or third-party service provider has obtained prior consent from any consumer whose personal information will be:
    - (a) Used in connection with an additional permitted ~~transactionactivity~~, as defined in this Act; or
    - (b) Shared with a person outside the jurisdiction of the United States, or its territories, as provided in this Act.

- B. Consistent with the requirements of this Act, a licensee may collect, process, retain, or share a consumer's personal information in connection with an insurance transaction as necessary:
- (1) For the servicing of any insurance application, policy, contract, or certificate under which the consumer is an actual or prospective insured, claimant, or beneficiary;
  - (2) For compliance with a legal obligation to which the licensee is subject;
  - (3) For compliance with a request or directive from a law enforcement or insurance regulatory authority;
  - (4) For compliance with a warrant, subpoena, discovery request, judicial order, or other administrative, criminal, or civil legal process, or any other legal requirement that is binding upon the licensee collecting, processing, retaining, or sharing the personal information;

**Commented [KJ32]:** Most of these requirements were taken from Model 670 Section 13 with some additional restrictions on sharing and processing.

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (5) For a lienholder, mortgagee, assignee, lessor, or other person shown on the records of an insurer or producer as having a legal or beneficial interest in a policy of insurance, to protect that interest provided that:
- (a) No health information is shared unless the sharing would otherwise be permitted by this section, and
  - (b) The information shared is limited to that which is reasonably necessary to permit such person to protect its interests in such policy;
- (6) To enable a licensee to detect or prevent criminal activity, fraud, material misrepresentation, or material nondisclosure in connection with an insurance transaction;
- (7) To enable a health care provider to:
- (a) Verify the consumer's insurance coverage or benefits;
  - (b) Inform a consumer of health information of which the consumer may not be aware; or
  - (c) Conduct an operations or services audit to verify the individuals treated by the health care provider; provided only such information is shared as is reasonably necessary to accomplish the audit;
- (8) To permit a party or a representative of a party to a proposed or consummated sale, transfer, merger or consolidation of all or part of the business of the licensee to review the information necessary for such transaction, provided:
- (a) Prior to the consummation of the sale, transfer, merger, or consolidation only such information is shared as is reasonably necessary to enable the recipient to make business decisions about the purchase, transfer, merger, or consolidation; and
  - (b) The recipient agrees not to share consumers' personal information until:
    - (i) consumer privacy protection notices have been provided to the consumers and
    - (ii) the recipient has complied with the provisions of this Act;
- (9) For an affiliate whose only use of the information is to perform an audit of a licensee provided the affiliate agrees not to process personal information for any other purpose or to share the personal information;
- (10) To permit a group policyholder to report claims experience or conduct an audit of the operations or services of a licensee, provided the information shared is reasonably necessary for the group policyholder to make the report or conduct the audit and is not otherwise shared; or

Commented [KJ33]: More restrictive than Model 670

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (11) To permit (i) a professional peer review organization to review the service or conduct of a healthcare provider provided the personal information is not otherwise processed or shared or (ii) to permit arbitration entities to conduct an arbitration related to a consumer's claim;
  - (12) To provide information to a consumer regarding the status of an insurance transaction; or
  - (13) To permit a governmental authority to determine the consumer's eligibility for health care benefits for which the governmental authority may be liable.
- C. No licensee shall, unless legally required, collect, process, retain, or share a consumer's personal information with an entity outside of the United States and its territories, unless the licensee has provided the required notice and obtained the consumer's prior express consent to do so, as required by Article III of this Act.
- D. No licensee shall permit any of its officers, employees, or agents to collect, process, retain, or share any consumer's personal information, except as relevant and necessary as part of that person's assigned duties.
- E. No licensee may collect, process, retain, or share a consumer's personal information in connection with any additional permitted ~~transactions-activities~~ without consumers' prior express consent. Once consent has been given, any person may conduct marketing, actuarial studies, and research activities as follows:
- (1) For actuarial studies and research activities:
    - (a) No consumer may be identified in any research study or report;
    - (b) All materials allowing the consumer to be identified are returned to the licensee that initiated the actuarial or research study; and
    - (c) A consumer's personal information is deleted as soon as the information is no longer needed for the specific actuarial or research study.
  - (2) For all additional permitted ~~transactions-activities~~:
    - (a) The person conducting the marketing, actuarial study, or research activity agrees not to further share any consumer's personal information; and
    - (b) A consumer's sensitive personal information may not be shared or otherwise provided to any person for use in connection with any additional permitted ~~transactionactivity~~.
- F. A licensee may collect, process, retain, or share consumers' de-identified personal information.
- G. No licensee shall:

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (1) Collect, process, retain, or share personal information in a manner inconsistent with the direction of a consumer pursuant to this act; or
- (2) Collect, process, retain, or share personal information in a manner requiring the prior express consent or authorization of the consumer without obtaining such prior consent.

~~H. Notwithstanding any other provision of law, no licensee may sell or share consumers' personal information for any type of consideration.~~

- I. This section shall not prohibit the collection, processing, retention, or sharing of consumers' personal information to the extent preempted by subdivisions (b)(1)(H) or (b)(2) of Section 625 of the Fair Credit Reporting Act.

### Section 5. Retention and Deletion of Consumers' Information

- A. Once the initial consumer privacy protections notice has been provided to the consumer as set forth in this Act, a licensee may retain a consumer's personal information as necessary for:
  - (1) The servicing of an insurance application, policy, contract, or certificate under which the consumer is an actual or prospective insured, claimant, or beneficiary;
  - (2) Compliance with a legal obligation applicable to any insurance transaction involving consumers' personal information to which the licensee is subject;
  - (3) Compliance with a request or directive from a law enforcement or insurance regulatory authority;
  - (4) Compliance with a warrant, subpoena, discovery request, judicial order, or other administrative, criminal, or civil legal process, or other legal requirement that is binding upon a licensee in connection with consumers' personal information;
  - (5) Protection of a legal or beneficial interest in a policy of insurance, with respect to a lienholder, mortgagee, assignee, lessor, or other person shown on the records of an insurer or producer as having a legal or beneficial interest in the policy;
  - (6) Any record retention requirements under any state or federal law applicable to any insurance transaction involving consumers' personal information;
  - (7) Any statute of limitation periods under any state or federal law applicable to any insurance transaction involving consumers' personal information; or

**Insurance Consumer Privacy Protection Model Law #674**

**2023 Privacy Protections Working Group**

- (8) Any additional permitted ~~transaction-activity~~ provided the consumer has consented in writing to the use of the consumer's personal information for this purpose, the licensee may retain consumer's personal information for as long as the consumer's consent to an additional permitted ~~transaction-activity~~ has not been revoked pursuant to Section 9 of this Act.
- B. Once the provisions of Subsection A of this section are no longer applicable to any of a consumer's personal information held by a licensee:
  - (1) Such licensee shall completely delete all the consumer's personal information within 90 days after the provisions in Subsection A of this section no longer apply.
  - (2) Any third-party service provider in possession of the consumer's personal information shall notify the licensee that the consumer's information has been completely deleted.
  - (3) If the licensee no longer has a relationship with the consumer in connection with any insurance transactions, the licensee shall send a notice to the consumer informing the consumer that:
    - (a) The licensee and any third-party service providers no longer retain any of the consumer's personal information and
    - (b) The annual Notice of Consumer Privacy Protections required by Article III of this Act will no longer be sent to the consumer.
  - (4) A licensee shall develop policies and procedures for compliance with this section and be able to demonstrate compliance with those policies and procedures.



## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

#### ARTICLE III. NOTICES AND AUTHORIZATIONS

##### Section 6. Initial and Annual Notice of Consumer Information Practices

- A. A licensee that collects, processes, retains, or shares a consumer's personal information in connection with insurance transactions, by whatever means used, shall provide to consumers clear and conspicuous notices that accurately reflect its information policies and practices.
- B. An initial consumer information practices notice shall be provided to a consumer before the licensee, directly or through a third-party service provider, first does any of the following:
- (1) Collects, processes, retains, or shares the consumer's personal information in connection with an application for insurance coverage;
  - (2) Collects, processes, retains, or shares the consumer's personal information in connection with a claim under an insurance policy;
  - (3) Collects the consumer's personal information from a source other than the consumer or public records;
  - (4) Collects, processes, retains, or shares the consumer's personal information in connection with value-added services;
  - (5) Collects, processes, or shares the consumer's personal information in connection with an additional permitted ~~transaction~~activity; or
  - (6) Collects, processes, or shares the consumer's personal information, including but not limited to reviewing the consumer's policy or coverage for renewal or reinstatement, if the consumer relationship predates the applicability of this section and the consumer has not already received a notice substantially similar notice.
- C. A further information practice notice shall be provided not less than annually to each consumer with whom the licensee has an ongoing business relationship. The licensee shall conspicuously identify any material changes in its information practices.
- D. The licensee shall honor all representations made to consumers in its most current initial and annual notices, unless otherwise compelled by law, in which case the licensee shall promptly send a notice to all affected consumers explaining the changes in the licensee's information practices. If the licensee's information practices change, the licensee remains bound by the terms of the most recent notice it has given a consumer, until a revised notice has been given.
- E. When a licensee is required to provide a consumer a consent form required by this Act, the licensee shall deliver it according to Section 8.

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

#### Section 7. Content of Consumer Information Practices Notices

- A. The content of any notice required by Section 6 shall state in writing all of the following:
- (1) Whether personal information has been or may be collected from any sources other than the consumer or consumers proposed for coverage, and whether such information is collected by the licensee or by a third-party service provider;
  - (2) The specific types of personal information of the consumer that the licensee or any of its third-party service providers has or may collect, process, retain, or share;
  - (3) The specific purposes for which the licensee collects, processes, retains, or shares personal information as permitted by this Act;
  - (4) The sources that have been used or may be used by the licensee to collect, process, retain, or share the consumer's personal information;
  - (5) That consumers' personal information may be shared for any of the purposes listed permitted in this Act, or a description of the licensee's information practices if those practices are more limited than permitted by this Act;
  - (6) That the consumer may, upon request, obtain a list of any persons with which the licensee or any of the licensee's third-party service providers has shared the consumer's personal information within the current calendar year and, at a minimum, the three previous calendar years.
  - (7) A description of the following requirements as established under Section 4 of this Act:
    - (a) The requirement that the licensee or third-party service provider obtain the consumer's express written consent prior to sharing the consumer's personal information with any person in connection with the collection, processing, retention, or sharing of the consumer's personal information with a person in a jurisdiction outside of the United States and its territories; and the consumer's right to prohibit sharing of the consumer's personal information with such a person;
    - (b) The requirement that the licensee obtain the consumer's express written consent for the collection, processing, retention, or sharing of a consumer's personal information for actuarial purposes unless such information has been de-identified;

Commented [KJ34]: This is language is consistent with Model 910 (Record Retention)

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (c) The requirement that the licensee obtain the consumer's express written consent for the collection, processing, retention, or sharing of a consumer's personal information for research purposes unless such information has been de-identified; and
- (d) The requirement for the licensee to obtain the consumer's express written consent for the collection, processing, retention, or sharing of a consumer's personal information for marketing a product or service to the consumer;
- (8) A description of the rights of the consumer to access, correct or amend personal information about the consumer and to correct or amend factually incorrect personal information as established under Article IV of this Act, and the instructions for exercising such rights ;
- (9) A statement of the rights of non-retaliation established under Section 13 of this Act;
- (10) A summary of the reasons the licensee or any third-party service provider retains personal information and the approximate period of retention; and
- (11) A statement that no licensee or third-party service provider may sell or share for valuable consideration a consumer's personal information.
- (12) In addition to the notice provided to consumers, a licensee shall prominently post and make available the notice required by this section on its website, if a website is maintained by the licensee. ~~The licensee shall design its website notice as follows:~~
  - (a) The notice is clear and conspicuous;
  - (b) The licensee uses text or visual cues to encourage scrolling down the page, if necessary, to view the entire notice and ensure that other elements on the web site (such as text, graphics, hyperlinks, or sound) do not distract attention from the notice, and
  - (c) The licensee either:
    - (i) Places the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or
    - (ii) Places a link on a screen that consumers frequently access, such as a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature, and relevance of the notice.

Commented [KJ35]: This language is from Model 672

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- B. If the licensee uses a consumer's personal information to engage in additional permitted ~~transactions~~activities, in addition to the provisions in Subsection A of this section, the following information shall be included in the notice:
- (1) A statement that the consumer may, but is not required to, consent to the collection, processing, sharing, and retention of the consumer's personal information for any additional permitted ~~transactions~~activities in which the licensee engages;
  - (2) A description of the reasonable means by which the consumer may express written consent;
  - (3) That the consumer may consent to any one or more of the additional permitted ~~transactions~~activities or refuse to consent to any one or more of the additional permitted ~~transactions~~activities;
  - (4) That once consent has been given for an additional permitted ~~transaction~~activity, the consumer may revoke consent at any time;
  - (5) That once consent for using a consumer's personal information for an additional permitted ~~transaction~~activity is withdrawn, the licensee will no longer engage in such additional permitted ~~transaction~~activity using the consumer's personal information; and
  - (6) That once consent to an additional permitted ~~transaction~~activity has been revoked, any of the consumer's personal information in the possession of the licensee used solely for that additional permitted ~~transaction~~activity will be destroyed and deleted as set forth in Section 5 of this Act.
- C. If the licensee shares consumers' personal information with a person who will collect, process, retain, or share consumers' personal information in a jurisdiction outside of the United States and its territories, the following information shall additionally be included in any notice required by Section 6 of this Act:
- (1) A statement that the consumer may, but is not required to, consent to the collection, processing, retention, or sharing, of the consumer's personal information a jurisdiction outside of the United States and its territories;
  - (2) A description of the reasonable means by which the consumer may express written consent;
  - (3) That once consent has been given for the collection, processing, retention, or sharing of consumers' personal information in a jurisdiction outside the United States and its territories, a consumer may revoke consent at any time; and
  - (4) That once consent for the collection, processing, retention, or sharing of consumers' personal information by a person in a jurisdiction outside the United States and its territories has been revoked, any of the consumer's

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

personal information in the possession of such person shall be deleted as set forth in Section 5 of this Act.

- E. The obligations imposed by this section upon a licensee may be satisfied by another licensee or third-party service provider authorized to act on its behalf.

#### Section 8. Delivery of Notices Required by This Act

Commented [KJ36]: This language comes from Model 672

- A. A licensee shall provide any notices required by this Act so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, electronically pursuant to [state's UETA law].
- B. A licensee may reasonably expect that a consumer will receive actual notice if the licensee:
- (1) Hand-delivers a printed copy of the notice to the consumer;
  - (2) Mails a printed copy of the notice to the address of record of the consumer separately, or in a policy, billing, or other written communication;
  - (3) For a consumer who has agreed to conduct transactions electronically, posts the notice on the electronic site and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular insurance product or service or emails the notice to the consumer and requests a delivery receipt ;
- C. A licensee may not, however, reasonably expect that a consumer will receive actual notice of its privacy policies and practices if it:
- (1) Only posts a sign in its office or generally publishes advertisements of its privacy policies and practices; or
  - (2) Sends the notice electronically to a consumer who has not agreed to conduct business electronically with the licensee in connection with an insurance transaction or an additional permitted transactionactivity.
  - (3) Sends the notice electronically to a consumer who has agreed to conduct business electronically with the licensee in connection with an insurance transaction or an additional permitted transactionactivity, but the licensee does not obtain a delivery receipt.
- D. A licensee may reasonably expect that a consumer will receive actual notice of the licensee's annual privacy notice if:
- (1) The consumer uses the licensee's web site to access insurance products and services electronically and agrees to receive notices at the web site and the licensee posts its current privacy notice continuously in a clear and conspicuous manner on the web site; or

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (2) The licensee mails or emails the notice to the consumer's address of record.
  - (3) A licensee may not provide any notice required by this Act solely by orally explaining the notice, either in person or over the telephone.
  - (4) The licensee provides all notices required by this Act so that the consumer can retain them or obtain them later in writing or, if the consumer agrees, electronically.
- E. A licensee may provide a joint notice from the licensee and one or more of its affiliates if the notice accurately reflects the licensee's and the affiliate's privacy practices with respect to the consumer.
- F. If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may satisfy the initial and annual notice requirements of Sections 6 and 7 of this Act, respectively, by providing one notice to those consumers jointly. The notice must reflect the consent of each consumer.
- G. If any consumer has requested that the licensee refrain from sending an annual notice of consumer privacy protections and the licensee's current privacy protections notice remains available to the consumer upon request, the licensee shall honor the consumer's request but must continue to send any jointly insured consumer the annual notice.

### Section 9. Consumers' Consent- How Obtained

- A. Where the consumer's consent for the collection, processing, or sharing of consumers' personal information by a licensee is required by this Act, a licensee shall provide a reasonable means to obtain written consent and maintain a written record of such consent.
- (2) A licensee may provide the consent form together with or on the same written or electronic form as the most recent of the initial or annual notice the licensee provides in accordance with Section 6.
  - (3) If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may provide a single consent notice. Each of the joint consumers may consent or refuse to consent.
  - (4) A licensee does not provide a reasonable means of obtaining express written consent if consent is required or the consumer is instructed that consent is required.
  - (5) A licensee shall comply with a consumer's consent directive as soon as reasonably practicable after the licensee receives it.

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (7) Any consumer who has given consent for the use of personal information in connection with additional permitted ~~transactions~~activities, may revoke consent for collection, processing, retention, or sharing of such consumer's personal information. A consumer may exercise the right to consent or to withdraw consent at any time.
  - (8)
    - (a) A consumer's consent directive under this section is effective until the consumer revokes it in writing.
    - (b) If the consumer subsequently establishes a new relationship with the licensee, the consent directive for any specific activity that applied to the former relationship does not apply to the new relationship. A new relationship occurs when the consumer who previously ended all business relationships with the licensee re-establishes a business relationship more than thirty (30) days after the previous business relationship ended.
  - (9) If the consumer has made conflicting directives pursuant to this section, the consumer's most recent directive for the specific activity shall take precedence.
  - (10) Contracts between a licensee and any third-party service providers shall require either entity receiving to honor the consumer's directive pursuant to this section, and to refrain from collecting, processing, retaining, or sharing the consumer's personal information in a manner inconsistent with the directive of the consumer.
- B. When requesting a consumer's consent to use the consumer's personal information for actuarial studies conducted by a person other than the licensee, or research or marketing activities by anyone, as required by this Act, the consent request shall:
- (1) Be clear and conspicuous;
  - (2) Explain, in plain language, that consent is being sought to use the consumer's personal information for actuarial studies by a person other than the licensee, or for research or marketing activities;
  - (3) Permit the consumer to separately provide consent for use of the consumer's personal information other than sensitive personal information for any one or more additional permitted ~~transactions~~activities;
  - (4) Explain, in plain language, that the consumer is not required to provide consent to use the consumer's personal information for any one or all these purposes, and that the consumer will not be subject to retaliation or discrimination as outlined in Section 13, based on the consumer's choice; and
  - (5) State that use of a consumer's sensitive personal information for marketing purposes is prohibited.

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (6) The provisions of Subsection B of this section do not apply to consumers' personal or privileged information that has been de-identified in accordance with this Act.

#### Section 10. Content of Authorizations

Commented [KJ37]: Language from Model 670

- A. No person shall use an authorization for the collection, processing, or sharing of a consumer's personal or privileged information in connection with an insurance transaction unless the authorization meets following requirements.
- (1) Is written in plain language;
  - (2) Is dated and contains an expiration date for the consent;
  - (3) Specifies the persons authorized to collect, process, or share the consumer's personal or privileged information consistent with the provisions of this Act;
  - (4) Specifies the specific and explicit purposes for which the consumer's personal or privileged information is authorized to be collected, processed, or shared as permitted in Article II of this Act;
  - (5) Names the licensee whom the consumer is authorizing to collect, process, or share the consumer's personal or privileged information;
  - (6) Advises the consumer that they are entitled to receive a copy of the authorization.
- B. No authorization signed by a consumer shall be valid for longer than:
- (1) For an authorization signed for the purpose of collecting, processing, or sharing a consumer's personal or privileged information in connection with an application for insurance, a reinstatement of an insurance policy, or a request for change in insurance benefits:
    - (a) Twenty-four (24) months from the date the authorization is signed if the application or request involves life, health, or disability insurance; or
    - (b) Ninety (90) days from the date the authorization is signed if the application or request involves property or casualty insurance;
  - (2) For an authorization signed for the purpose of collecting, processing, or sharing a consumer's personal or privileged information in connection with a claim for benefits under an insurance policy, for the duration of the claim.



## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (3) For an authorization signed for the purpose of collecting, processing, or sharing a consumer's personal information in connection with loss prevention under an insurance policy, for the duration of the product or service.
- (4) For an authorization signed for the purpose of collecting, processing, or sharing a consumer's personal information in connection with an additional permitted ~~transaction~~ activity, no longer than 12 months.

**Drafting Note:** The standard established by this section for disclosure authorization forms is intended to supersede any existing requirements a state may have adopted even if such requirements are more specific or applicable to particular authorizations such as medical information authorizations. This section is intended to be the exclusive statutory standard for all authorization forms utilized by licensees. This section does not preclude the inclusion of a disclosure authorization in an application form nor invalidate any disclosure authorizations in effect prior to the effective date of this Act. Nor does this section preclude a licensee from obtaining, in addition to its own authorization form which complies with this section, an additional authorization form required by the person from whom disclosure is sought.

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

#### ARTICLE IV. CONSUMERS' RIGHTS

##### Section 11. Access to Personal Information

- A. Any consumer, after proper identification, may submit a written request to a licensee for access to the consumer's personal information in the possession of the licensee.
- B. The licensee or any third-party service provider shall
- (1) Acknowledge the request within five (5) business days; and
  - (2) Within fifteen (15) business days from the date such request is received:
    - (a) Disclose to the consumer the identity of those persons to whom the licensee or any third-party service provider has shared the consumer's personal information ~~within the current year and, at a minimum, the three~~ calendar years prior to the date the consumer's request is received.
    - (b) Provide the consumer with a summary of the consumer's personal information and the process for the consumer to request a copy of such information in the possession of the licensee.
    - (c) Identify the source of any consumer's personal information provided to the consumer pursuant to this subsection.
- C. Personal health information in the possession of licensee and requested under Subsection A of this section, together with the identity of the source of such information, shall be supplied either directly to the consumer or as designated by the consumer, to a health care provider who is licensed to provide medical care with respect to the condition to which the information relates. If the consumer elects for the licensee to disclose the information to a health care provider designated by the consumer, the licensee shall notify the consumer, at the time of the disclosure, that it has provided the information to the designated health care provider.
- D. The obligations imposed by this section upon a licensee may be satisfied by another licensee authorized to act on its behalf.
- E. The rights granted to consumers in this section shall extend to any individual to the extent personal information about the individual is collected, processed, retained, or shared by a licensee or its third-party service provider in connection with an insurance transaction or an additional permitted ~~transaction~~activity.
- F. For purposes of this section, the term "third-party service provider" does not include "consumer reporting agency" except to the extent this section imposes more stringent requirements on a consumer reporting agency than other state or federal laws.
- G. The rights granted to any consumer by this subsection shall not extend to information about the consumer that is collected, processed, retained, or shared in

Commented [KJ38]: From Model 910

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

connection with, or in reasonable anticipation of, a claim or civil or criminal proceeding involving the consumer.

#### Section 12. Correction or Amendment of Personal Information

- A. Any consumer, after proper identification, may submit a written request to a licensee to correct or amend any personal information about the consumer within the possession of the licensee.
- B. The licensee or any third-party service provider shall
- (1) Acknowledge the request within five (5) business days; and
  - (2) Within fifteen (15) business days from the date such request is received:
    - (a) Correct or amend the personal information in dispute; or
    - (b) If there is a specific legal basis for not correcting or amending the personal information in question, the licensee or its third-party service provider may refuse to make such correction or amendment. However, the licensee refusing to take such action shall provide the following information to the consumer:
      - (i) Written notice of the refusal to make such correction or amendment;
      - (ii) The basis for the refusal to correct or amend the information;
      - (iii) The contact information for filing a complaint with the consumer's state insurance regulator, and
      - (iv) The consumer's right to file a written statement as provided in Subsection C of this section.
  - (3) No licensee may refuse to correct or amend a consumer's personal information without good cause, such cause shall be demonstrated to commissioner of the consumer's state insurance department, upon request.
- C. If the licensee corrects or amends personal information in accordance with Subsection A. (1) of this section, the licensee shall so notify the consumer in writing and furnish the correction or amendment to:
- (1) Any person specifically designated by the consumer who may have, received such personal information within the preceding two (2) years;
  - (2) Any insurance support organization whose primary source of personal information is insurers if the insurance support organization has systematically received such personal information from the insurer within the preceding five (5) years; provided, however, that the correction or amendment need not be

Commented [KJ39]: This section is from Model 670 with a shortening of the length of time for B 2

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

furnished if the insurance support organization no longer maintains personal information about the consumer;

(3) Any third-party service provider that furnished such personal information.

D. Whenever a consumer disagrees with the refusal of a licensee to correct or amend personal information, the consumer shall be permitted to file with the licensee a concise statement setting forth:

(1) The relevant and factual information that demonstrates the errors in the information held by the licensee; and

(2) The reasons why the consumer disagrees with the refusal of the licensee to correct or amend the personal information.

E. In the event a consumer files such statement described in Subsection C, the insurer, producer, or insurance support organizations shall:

(1) Include the statement with the disputed personal information and provide a copy of the consumer's statement to anyone reviewing the disputed personal information; and

(2) In any subsequent disclosure by the insurer, producer, or support organization of the personal information that is the subject of disagreement, clearly identify the matter or matters in dispute and include the consumer's statement with the personal information being disclosed.

F. The rights granted to a consumer by this subsection shall not extend to personal information about the consumer that is collected, processed, retained, or shared in connection with or in reasonable anticipation of a claim or civil or criminal proceeding involving the consumer.

G. For purposes of this section, the term "insurance support organization" does not include "consumer reporting agency" except to the extent that this section imposes more stringent requirements on a consumer reporting agency than other state or federal law.

### Section 13. Nondiscrimination and Nonretaliation

A. A licensee and third-party service providers shall not retaliate against a consumer because the consumer exercised any of the rights under this Act. There shall be a rebuttable presumption that a licensee or third-party service provider has discriminated or retaliated against a consumer if:

(1) The consumer is required to consent to an additional permitted ~~transaction-~~  
activity to obtain a particular product, coverage, rate, or service;

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (2) The consumer is required to consent to an additional permitted ~~transaction~~ activity in order to provide consent that is otherwise required to obtain an insurance transaction;
- (3) The consumer is required to consent to collection, processing, retention, or sharing of the consumer's information in a jurisdiction outside of the United States and its territories to obtain a particular product, coverage, rate, or service; or
- (4) The consumer is required to consent to collection, processing, retention, or sharing of the consumer's information in a jurisdiction outside of the United States and its territories in order to provide consent that is otherwise required to obtain an insurance transaction.

**Drafting Note:** This section is meant to incorporate similar provisions from Model 672 in this model.

- B. There shall be a rebuttable presumption that consistent with the licensee's filed rules, rates, and forms, and normal underwriting guidelines in the state in which the consumer resides, the following acts do not constitute discrimination or retaliation if the act is reasonably related to any change in price or quality of services or goods applicable to all customers if the licensee is an insurer or a producer, or if a third-party service provider:
  - (1) Charges a different rate or premium to the consumer;
  - (2) Provides a different insurance product,
  - (3) Refuses to write insurance coverage for the consumer; or
  - (4) Denies a claim under an insurance product purchased by the consumer.

**Insurance Consumer Privacy Protection Model Law #674**

2023 Privacy Protections Working Group

**ARTICLE V. ADVERSE UNDERWRITING DECISIONS; OTHER TRANSACTIONS [OPTIONAL]**

**Section 14. Adverse Underwriting Decisions**

**Commented [KJ40]:** The provisions in this section are largely from Model 670 with some amendments

- A. Notice of an adverse underwriting decision. In the event of an adverse underwriting decision the licensee responsible for the decision shall:
- (1) Either provide in writing to the consumer at the consumer's address of record:
    - (a) The specific reason or reasons for the adverse underwriting decision, or
    - (b) That upon written request the consumer may receive the specific reason or reasons for the adverse underwriting decision in writing; and
  - (2) Provide the consumer with a summary of the rights established under Subsection C of this Section and Sections 11 and 12 of this Act.

**Drafting Note:** Adverse underwriting decisions include: (i) an increase in the risk; (ii) increase in rates in geographical area; (iii) increase base rates; (iv) change in insurance credit score that causes an increase in the premium; (v) the consumer has lost a discount; (vi) an insured had a claim; (vii) a lapse in coverage.

- B. Upon receipt of a written request within ninety (90) business days from the date of a notice of an adverse underwriting decision was sent to a consumer's address of record, the licensee within ten (10) business days from the date of receipt of such request shall furnish to the consumer the following information in writing to the consumer's address of record:
- (1) The specific reason or reasons for the adverse insurance decision, if such information was not initially furnished pursuant to Subsection A(1);
  - (2) The specific information that supports those reasons, provided:
    - (a) A licensee shall not be required to furnish specific privileged information if it has a reasonable suspicion, based upon specific information available for review by the Commissioner, that the consumer has engaged in criminal activity, fraud, material misrepresentation or material nondisclosure, or
    - (b) Health information supplied by a health care provider shall be disclosed either directly to the consumer about whom the information relates or to a health care provider designated by the individual consumer and licensed to provide health care with respect to the condition to which the information relates.
  - (3) A summary of the rights established under Subsection C and Sections 11 and 12 of this Act; and

**Drafting Note:** The exception in Section 10B(2)(a) to the obligation of an insurance institution or agent to furnish the specific items of personal or privileged information that support the reasons for an adverse underwriting decision extends only to information about criminal activity, fraud, material misrepresentation or material nondisclosure that is privileged information and not to all information.

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (4) The names and addresses of the sources that supplied the information outlined in Subsection B(2); provided, however, that the identity of any health care provider shall be disclosed either directly to the consumer or to the health care provider designated by the consumer.
- C. The obligations imposed by this section upon a licensee may be satisfied by another licensee authorized to act on its behalf.

#### Section 15. Information Concerning Previous Adverse Underwriting Decisions

No licensee may make inquiries in connection with an insurance transaction concerning:

- A. Any previous adverse underwriting decision received by a consumer; or
- B. Any previous insurance coverage obtained by a consumer through a residual market mechanism;

unless such inquiries also request the reasons for any previous adverse underwriting decision or the reasons why insurance coverage was previously obtained through a residual market mechanism.

#### Section 16. Previous Adverse Underwriting Decisions

No licensee may base an adverse underwriting decision in whole or in part on any of the following:

- A. A previous adverse underwriting decision or that a consumer previously obtained insurance coverage through a residual market mechanism. However, an insurer or producer may base an adverse underwriting decision on further information obtained from a licensee responsible for a previous adverse underwriting decision;
- B. Personal information received from third-party service providers whose primary source of information is insurers. However, a licensee may base an adverse underwriting decision on further supporting information obtained from a third-party service provider; or
- C. Solely on the loss history of the previous owner of the property to be insured.

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

#### ARTICLE VI. ADDITIONAL PROVISIONS

##### Section 17. Pretext Interviews [OPTIONAL]

No licensee shall use or authorize the use of pretext interviews to obtain information in connection with an insurance transaction; provided, however, that a pretext interview may be undertaken to obtain information from an individual or legal entity that does not have a generally or statutorily recognized privileged relationship with the consumer about whom the information relates to investigate a claim where, based upon specific information available for review by the Commissioner, there is a reasonable basis for suspecting criminal activity, fraud, material misrepresentation, or material nondisclosure in connection with the claim.

**Drafting Note:** Some states may desire to eliminate the exception in this section and thereby prohibit pretext interviews in all instances. Other states may desire to broaden the exception so that pretext interviews can be utilized in underwriting and rating situations as well as claim situations. States may either expand or limit the prohibition against pretext interviews suggested in this section to accommodate their individual needs and circumstances. Deviation from the standard developed here should not seriously undermine efforts to achieve uniform rules for insurance consumer privacy protections throughout the various states.

##### Section 18. Investigative Consumer Reports [OPTIONAL]

- A. No licensee may prepare or request an investigative consumer report about a consumer in connection with an insurance transaction involving an application for insurance, a policy renewal, a policy reinstatement, or a change in insurance benefits unless the licensee informs the consumer in writing prior to the report being prepared that the consumer:
- (1) May request to be interviewed in connection with the preparation of the investigative consumer report; and
  - (2) Is entitled to receive a copy of the investigative consumer report.
- B. If a licensee prepares an investigative consumer report, the insurer or producer shall conduct a personal interview of a consumer if requested by that consumer.
- C. If a licensee requests a third-party service provider to prepare an investigative consumer report, the licensee requesting such report shall notify in writing the third-party service provider whether a personal interview has been requested by the consumer. The third-party service provider shall conduct the interview requested.
- D. The licensee shall provide a written copy of the investigative consumer report to the consumer.
- E. Notwithstanding Subsections A through D of this section, any licensee that prepares or requests an investigative consumer report in connection with an insurance claim shall notify the consumer that the consumer may request to be interviewed in connection with the preparation of the investigative consumer report. However,

Commented [K41]: This language with modifications for clarity came from Model 67.0



## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

neither the licensee nor the third-party service provider is required to provide a copy of an investigative report prepared in connection with an insurance claim unless compelled to do so by a state or federal court.

#### Section 19. Compliance with HIPAA and HITECH

- A. A licensee that is subject to and compliant with the privacy and notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, HITECH), and collects, processes, retains, and shares all personal information in the same manner as protected health information:
- (1) Shall be deemed to comply with Sections 4-8 of this Act provided:
    - (a) The licensee obtains the consent of the consumer prior to engaging in any additional permitted ~~transactions~~activities; as defined in this Act; and
    - (b) The licensee obtains all necessary consent of consumers' whose personal information is shared with a person outside the jurisdiction of the United States or its territories, as provided in this Act; and
  - (2) Must comply with the remaining sections of this Act, as applicable.
- B. The licensee shall submit to the [Commissioner] a written statement certifying that the licensee comply with the requirements of Subsections A of this section.
- C. Subsections A and B of this section apply to such licensee if the [Commissioner] has not issued a determination finding that the applicable federal regulations are materially less stringent than the requirements of this Act and if the licensee has complied with the requirements of this section.

**Insurance Consumer Privacy Protection Model Law #674**

**2023 Privacy Protections Working Group**

**ARTICLE VII GENERAL PROVISIONS**

**Section 20. Power of Commissioner**

- A. The Commissioner shall have power to examine and investigate into the affairs of every licensee doing business in this state to determine whether such licensee has been or is engaged in any conduct in violation of this Act.
- B. The Commissioner shall have the power to examine and investigate the affairs of every insurance support organization acting on behalf of a licensee that either transacts business in this state or transacts business outside this state that affects a person residing in this state to determine whether such insurance support organization has been or is engaged in any conduct in violation of this Act.

Commented [KJ42]: This language comes from Model 670

**Drafting Note:** Section 21 B is optional. The drafters included this language for those states that had already adopted Model 670 and those states that wish to adopt this provision.

**Section 21. Confidentiality**

Commented [KJ43]: This language was taken from Model 668 and modified for the purposes of this model.

- A. Any documents, materials or other information in the control or possession of the Insurance Department that are furnished by a licensee, third-party service provider, or an employee or agent thereof acting on behalf of the licensee pursuant to this Act, or that are obtained by the Commissioner in an investigation or examination pursuant to [Code Section] shall be confidential by law and privileged, shall not be subject to [insert reference to state open records, freedom of information, sunshine or other appropriate law], shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action. However, the Commissioner is authorized to use the documents, materials, or other information in the furtherance of any regulatory or legal action brought as a part of the Commissioner's duties.
- B. Neither the Commissioner nor any person who received documents, materials or other information while acting under the authority of the Commissioner shall be permitted or required to testify in any private civil action concerning any confidential documents, materials, or information subject to this Act.
- C. To assist in the performance of the Commissioner's duties under this Act, the Commissioner may:
  - (1) Share documents, materials or other information, including the confidential and privileged documents, materials or information subject to this Act, with other state, federal, and international regulatory agencies, with the National Association of Insurance Commissioners, its affiliates or subsidiaries, and with state, federal, and international law enforcement authorities, provided that the recipient agrees in writing to maintain the confidentiality and privileged status of the document, material, or other information;
  - (2) Receive documents, materials, or information, including otherwise confidential and privileged documents, materials, or information, from the National

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

Association of Insurance Commissioners, its affiliates or subsidiaries and from regulatory and law enforcement officials of other foreign or domestic jurisdictions, and shall maintain as confidential or privileged any document, material or information received with notice or the understanding that it is confidential or privileged under the laws of the jurisdiction that is the source of the document, material or information;

- (3) Share documents, materials, or other information subject to this Act, with a third-party consultant or vendor provided the consultant agrees in writing to maintain the confidentiality and privileged status of the document, material, or other information; and
  - (4) Enter into agreements governing sharing and use of information consistent with this subsection.
- D. No waiver of any applicable privilege or claim of confidentiality in the documents, materials, or information shall occur due to disclosure to the Commissioner under this section or due to sharing as authorized in this section.
- E. Nothing in this Act shall prohibit the Commissioner from releasing final, adjudicated actions that are open to public inspection pursuant to [insert appropriate reference to state law] to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates, or subsidiaries.

### Section 22 Record Retention

- A. Notwithstanding any other provision of law, a licensee shall maintain sufficient evidence in its records of compliance with this Act for the calendar year in which the activities governed by this Act occurred and the three calendar years thereafter.
- B. Additionally, a licensee or third-party service provider shall maintain all records necessary for compliance with the requirements of this Act, including, but not limited to:
- (1) Records related to the consumer's right of access pursuant to Article IV;
  - (2) Copies of authorizations and consent\ executed by any consumer pursuant to this Act, for as long as the consumer is in a continuing business relationship with the licensee; and
  - (3) Representative samples of any notice required to be provided to any consumer pursuant to this Act, for as long as the consumer is in a continuing business relationship with the licensee.

Commented [KJ44]: Language from Model 910

### Section 23. Hearings, Records, and Service of Process

Whenever the Commissioner has reason to believe that a licensee or its third-party service providers have been or are engaged in conduct in this state which violates this Act, or if the

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

Commissioner believes that a third-party service provider has been or is engaged in conduct outside this state that affects a person residing in this state and that violates this Act], the Commissioner shall issue and serve upon such a licensee or its third-party service provider a statement of charges and notice of hearing to be held at a time and place fixed in the notice. The date for such hearing shall be not less than [insert number] days after the date of service.

- A. At the time and place fixed for such hearing a licensee or its third-party service provider[, or third-party service provider] charged shall have an opportunity to answer the charges against it and present evidence on its behalf. Upon good cause shown, the Commissioner shall permit any adversely affected person to intervene, appear and be heard at such hearing by counsel or in person.
- B. At any hearing conducted pursuant to this section the Commissioner may administer oaths, examine, and cross-examine witnesses and receive oral and documentary evidence. The Commissioner shall have the power to subpoena witnesses, compel their attendance and require the production of books, papers, records, correspondence and other documents, and data that are relevant to the hearing. A record of the hearing shall be made upon the request of any party or at the discretion of the Commissioner. If no record is made and if judicial review is sought, the Commissioner shall prepare a statement of the evidence for use on the review. Hearings conducted under this section shall be governed by the same rules of evidence and procedure applicable to administrative proceedings conducted under the laws of this state.
- C. Statements of charges, notices, orders, and other processes of the Commissioner under this Act may be served by anyone duly authorized to act on behalf of the Commissioner. Service of process may be completed in the manner provided by law for service of process in civil actions or by registered or certified mail. A copy of the statement of charges, notice, order, or other process shall be provided to the person or persons whose rights under this Act have been allegedly violated. A verified return setting forth the manner of service or return receipt in the case of registered or certified mail, shall be sufficient proof of service.

**Drafting Note:** Consideration should be given to the practice and procedure in each state. The items in [] are optional and dependent on the state's authority.

#### Section 24. Service of Process -Third-Party Service Providers

For purposes of this Act, a third-party service provider transacting business outside this state that affects a person residing in this state shall be deemed to have appointed the Commissioner to accept service of process on its behalf; provided the Commissioner causes a copy of such service to be mailed forthwith by registered or certified mail to the third-party

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

service provider at its last known principal place of business. The return receipt for such mailing shall be sufficient proof that the same was properly mailed by the Commissioner.

#### Section 25. Cease and Desist Orders and Reports

- A. If, after a hearing pursuant to Section 23, the Commissioner determines that licensee or its third-party service provider charged has engaged in conduct or practices in violation of this Act, the Commissioner shall reduce his or her findings to writing and shall issue and cause to be served upon such licensee or its third-party service provider a copy of such findings and an order requiring such licensee or its third-party service provider to cease and desist from the conduct or practices constituting a violation of this Act.
- B. If, after a hearing, the Commissioner determines that the licensee or its third-party service provider charged has not engaged in conduct or practices in violation of this Act, the Commissioner shall prepare a written report which sets forth findings of fact and conclusions of law. Such report shall be served upon the insurer, producer, or insurance support organization charged and upon the person or persons, if any, whose rights under this Act were allegedly violated.
- C. Until the expiration of the time allowed for filing a petition for review or until such petition is filed, whichever occurs first, the Commissioner may modify or set aside any order or report issued under this section. After the expiration of the time allowed for filing a petition for review, if no such petition has been duly filed, the Commissioner may, after notice and opportunity for hearing, alter, modify, or set aside, in whole or in part, any order or report issued under this section whenever conditions of fact or law warrant such action or if the public interest so requires.

**Drafting Note:** Consideration should be given to the practice and procedure in each state.

#### Section 26. Penalties

- A. In any case where a hearing pursuant to Section 23 results in the finding of a knowing violation of this Act, the Commissioner may, in addition to the issuance of a cease and desist order as prescribed in Section 25, order payment of a monetary penalty of not more than [dollar amount] for each violation but not to exceed [dollar] in the aggregate for multiple violations.
- B. Any person who violates a cease and desist order of the Commissioner may, after notice and hearing and upon order of the Commissioner, be subject to one or more of the following penalties, at the discretion of the Commissioner:
  - (1) A monetary penalty of not more than [dollar amount] for each violation;

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (2) A monetary penalty of not more than [dollar amount] if the Commissioner finds that violations have occurred with such frequency as to constitute a general business practice; or
- (3) Suspension or revocation of the license of a licensee.

**Drafting Note:** Consideration should be given to the practice and procedure requirements and penalty requirements in each state.

#### Section 27. Judicial Review of Orders and Reports

- A. Any person subject to an order of the Commissioner under [Code cite] or any person whose rights under this Act were allegedly violated may obtain a review of any order or report of the Commissioner by filing in the [insert title] Court of [insert county] County, within [insert number] days from the date of the service of such order or report, a written petition requesting that the order or report of the Commissioner be set aside. A copy of such petition shall be simultaneously served upon the Commissioner, who shall certify and file in such court the entire record of the proceeding giving rise to the order or report which is the subject of the petition. Upon filing of the petition and record the [insert title] Court shall have jurisdiction to make and enter a decree modifying, affirming, or reversing any order or report of the Commissioner, in whole or in part. The findings of the Commissioner as to the facts supporting any order or report, if supported by clear and convincing evidence, shall be conclusive.
- B. To the extent an order or report of the Commissioner is affirmed, the Court shall issue its own order commanding obedience to the terms of the order or report of the Commissioner. If any party affected by an order or report of the Commissioner shall apply to the court for leave to produce additional evidence and shall show to the satisfaction of the court that such additional evidence is material and that there are reasonable grounds for the failure to produce such evidence in prior proceedings, the court may order such additional evidence to be taken before the Commissioner in such manner and upon such terms and conditions as the court may deem proper. The Commissioner may modify his or her findings of fact or make new findings by reason of the additional evidence so taken and shall file such modified or new findings along with any recommendation, if any, for the modification or revocation of a previous order or report. If supported by clear and convincing evidence, the modified or new findings shall be conclusive as to the matters contained therein.
- C. An order or report issued by the Commissioner shall become final:
  - (1) Upon the expiration of the time allowed for the filing of a petition for review, if no such petition has been duly filed; except that the Commissioner may modify or set aside an order or report; or

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

- (2) Upon a final decision of the [insert title] Court if the court directs that the order or report of the Commissioner be affirmed or the petition for review dismissed.
- D. No order or report of the Commissioner under this Act or order of a court to enforce the same shall in any way relieve or absolve any person affected by such order or report from any liability under any law of this state.

**Drafting Note:** Consideration should be given to the practice and procedure in each state.

#### ~~Section 28. Individual Remedies~~

##### ~~A. No Private Cause of Action [OPTIONAL].~~

~~Nothing in this Act shall be construed to create or imply a private cause of action for violation of its provisions, nor shall it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.~~

##### ~~B. Private Cause of Action [OPTIONAL].~~

- ~~(1) If a licensee or one or more of its third-party service providers fail to comply with this Act with respect to the rights granted under this Act, any person whose rights are violated may apply to the [insert title] Court of this state, or any other court of competent jurisdiction, for appropriate equitable relief.~~
- ~~(2) If a licensee or one or more of its third-party service provider discloses information in violation of this Act, the licensee shall be liable for damages sustained by the individual about whom the information relates; provided, however, that no individual shall be entitled to a monetary award which exceeds the actual damages sustained by the individual.~~
- ~~(3) In any action brought pursuant to this section, the court may award the cost of the action and reasonable attorney's fees to the prevailing party.~~
- ~~(4) An action under this section shall be brought within [two (2)] years from the date the alleged violation is or should have been discovered.~~
- ~~(5) Except as specifically provided in this section, there shall be no remedy or recovery available to individuals, in law or in equity, for occurrences constituting a violation of any provisions of this Act.~~
- ~~(6) No private cause of action may be brought unless there is an actual victim and actual damages. Damages sought shall be actual damages.~~
- ~~(7) No claim under this Act may be used to leverage class action litigation.~~

## Insurance Consumer Privacy Protection Model Law #674

### 2023 Privacy Protections Working Group

~~Drafting Note: Consideration should be given to the practice and procedure in each state. A state may choose to adopt either Section A or Section B or neither of these sections. However, adopting one or the other of these provisions makes it clearer what the consumers' rights are.~~

#### Section 29. Immunity

No cause of action in the nature of defamation, invasion of privacy or negligence shall arise against any person for disclosing personal or privileged information in accordance with this Act, nor shall such a cause of action arise against any person for furnishing personal or privileged information to an insurer, producer, or insurance support organization; provided, however, this section shall provide no immunity for disclosing or furnishing false information with malice or willful intent to injure any person.

#### Section 30. Obtaining Information Under False Pretenses

No person shall knowingly and willfully obtain information about a consumer from a licensee under false pretenses. A person found to be in violation of this section shall be fined not more than [insert dollar amount] or imprisoned for not more than [insert length of time], or both.

**Drafting Note:** This provision is applicable to states requiring this language.

#### Section 31. Severability

If any provisions of this Act or the application of the Act to any person or circumstance is for any reason held to be invalid, the remainder of the Act and the application of such provision to other persons or circumstances shall not be affected.

#### Section 32. Conflict with Other Laws

- A. All laws and parts of laws of this state inconsistent with this Act are hereby superseded with respect to matters covered by this Act.
- B. Nothing in this article shall preempt or supersede existing federal or state law related to health information.

#### Section 33. Rules and Regulations

The Commissioner may issue such rules, regulations, and orders as shall be necessary to carry out the provisions of this Act.



**Insurance Consumer Privacy Protection Model Law #674**

**2023 Privacy Protections Working Group**

**Section 34. Effective Date**

This Act shall take effect on [insert a date].



REINSURANCE ASSOCIATION OF AMERICA

April 3, 2023

Katie Johnson, Chair  
Privacy Protections (H) Working Group  
National Association of Insurance Commissioners  
c/o Ms. Lois Alexander  
Manager – Market Regulation  
Via email [lalexander@naic.org](mailto:lalexander@naic.org)

**Re: RAA Comments Regarding Exposure Draft of New *Consumer Privacy Protections Model Law #674***

Dear Ms. Johnson:

The Reinsurance Association of America (RAA) appreciates the opportunity to submit comments to the Privacy Protections (H) Working Group regarding the exposure draft of the *Consumer Privacy Protections Model Law (#674)*. The Reinsurance Association of America (RAA) is a national trade association representing reinsurance companies doing business in the United States. RAA membership is diverse, including reinsurance underwriters and intermediaries licensed in the U.S. and those that conduct business on a cross-border basis. The RAA also has life reinsurance affiliates and insurance-linked securities (ILS) fund managers and market participants that are engaged in the assumption of property/casualty risks. The RAA represents its members before state, federal and international bodies.

The RAA appreciates the Working Group's continued thoughtful engagement to update the model act. The RAA has identified a number of concerns with the exposure draft regarding its treatment of reinsurance. The RAA supports the concerns raised by our primary insurance colleagues and, rather than reiterating those comments, will focus our comments on reinsurance specific issues at this time. The RAA has three main concerns with the current draft: (1) reinsurers are not exempt from the requirements when the reinsurer is not collecting information from a consumer and has no direct interaction with a consumer; (2) the lack of clarity as to whether and the extent to which reinsurers would fall within the definitions of "insurers", "licensees", and/or "third-party service providers", which creates confusion as to how the law would apply to reinsurers and what their obligations would be under it; and (3) concerns regarding the restrictions on sharing data across international borders, which do not contemplate that reinsurance is a global and data-driven business.

Generally, the model inappropriately imposes requirements on reinsurers when there is no direct relationship between a reinsurer and a consumer. Reinsurers' customers are ceding insurance companies, not individuals who are insured by insurance companies. Laws and regulations should not create a customer or legal relationship between reinsurers and individuals. Creating this

relationship by imposing many of the requirements in the draft model on reinsurers is confusing to the consumer; would inappropriately interfere with the relationship between a consumer and the consumer's insurer; and could have significant unintended consequences regarding the operations of a reinsurer and the way reinsurers provide value to ceding companies and to the economy. As a result, many obligations in the model should not apply to reinsurers, particularly those pertaining to: all notice of information practices and other notice obligations; consumer consent; direct consumer rights requests; adverse underwriting decisions; pretext interviews and investigative consumer reports. Reinsurers should be exempt from these requirements. Providing an exemption would be consistent with the breach notice requirements under other privacy protection schemes, such as NYDFS Part 500, with the goal being to avoid inundating and confusing consumers with multiple notices. The current draft does not include such an exemption.

The RAA is also concerned at the lack of clarity with respect to whether and the extent to which reinsurers fall within the definitions of "insurer", "licensee", and/or "third-party service provider" under the current draft. As drafted, the definitions treat reinsurers inconsistently, including potential different treatment of foreign-domiciled reinsurers and domestic reinsurers. For example, under the definition of "insurer", reinsurers seem to be included under subsection (1), but subsection (4) exempts foreign-domiciled reinsurers. The definition of "licensee" seems to similarly exclude only assuming insurers domiciled in another state or jurisdiction. Lastly, even if reinsurers are not considered insurers or licensees, the broad definition of "third-party service provider" including "any person that obtains consumers' personal information from a licensee" could be read to include any reinsurer not falling within the definitions of insurer or licensee. The definitions require revision with respect to scope and application to reinsurers. The RAA is also concerned that the current definitions would put entities like (re)insurance brokers, considered both a "licensee" and "third-party service provider", at a double disadvantage for consent requirements, given the nature of their business and interactions with insurance companies. This is in contrast to all other key privacy laws which recognize different obligations for primary businesses than for service providers.

The RAA is also concerned about the cross-border restrictions that would pose significant challenges for the reinsurance industry, much of which operates globally. The RAA does not support the new proposed requirement mandating that an (re)insurer obtain consent from the customer if it shares or processes customer information outside the United States. This very significant restriction would impact a global reinsurers' ability to manage data within its own company that is located in another country. Reinsurance is a global business and restricting the ability to operate as such would have a significant impact on our members.

The RAA understands the efforts to amend this model will be ongoing for quite some time. The RAA appreciates the opportunity to work with you on this important project and specifically to address the reinsurance-specific concerns. We would be happy to meet with members of the Privacy Protections (H) Working Group and NAIC staff to discuss reinsurance operations and the regulation of reinsurance under state law. We look forward to further engagement on these issues.

Sincerely,

A handwritten signature in black ink that reads "Karalee C. Morell". The signature is written in a cursive style with a large, stylized 'K' and 'M'.

Karalee C. Morell  
SVP and General Counsel  
Reinsurance Association of America