

# Privacy of Consumer Financial and Health Information Regulation (#672)

## New Section 5 – Third Party Arrangements

Table of Contents - Public Comments Received (Due 9/18/24)

### Table of Contents

ACLI .....	1-5
AHIP.....	6-9
ALTA .....	10-11
APCIA .....	12-18
CA.....	19-35
CAI.....	36-40
Consumer Representatives.....	41-47
FL.....	48-49
IIABA.....	50-54
IRI .....	55-57
ME.....	58-61
NABIP .....	62-64
NAMIC .....	65-83
Next Insurance .....	84-85
PA .....	86-87
RAA .....	88-89
SD.....	90-91
BCBSA (received after due date – include, time permitting) .....	92
CCIA (received after due date – include, time permitting) .....	94

September 18, 2024

Commissioner Amy L. Beard, Chair  
Erica Weyhenmeyer, Vice Chair  
Privacy Protections (H) Working Group  
National Association of Insurance Commissioners  
1100 Walnut Street  
Kansas City, MO 64106-2197

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

*RE: ACLI Comments to Section 5 Third Party Arrangements to the Privacy Protections (H) Working Group*

Dear Chair Beard and Vice Chair Weyhenmeyer:

On behalf of the American Council of Life Insurers, we appreciate the opportunity to provide comments in response to the Chair's Draft revising Model 672, specifically focused on Section 5, Third Party Arrangements. ACLI and its members are appreciative of the collaborative and transparent process being undertaken by the Working Group and the continued opportunity for stakeholder input. ACLI members recognize their affirmative and continuing commitment to respect consumer privacy through transparency in the collection, use, and disclosure of personal information. ACLI members support reasonable consumer control over their personal information. Consumers have legitimate expectations that the personal information entrusted to and used by businesses will be kept confidential and secure. ACLI has been a collaborative and engaged industry leader and stakeholder throughout the PPWG's endeavor to update the Privacy Model. As such, we appreciate the opportunity to represent the Life Industry in the drafting group and look forward to continued dialogue.

Our comments on Section 5, Third Party Arrangements, and Recommended Changes to the Chair Draft Provisions are as follows:

### **Article II Section 5(A) Third Party Arrangements**

**Chair Draft Language:** "Contract Requirements. Consistent with the size and complexity of the third-party, a licensee that discloses a consumer's nonpublic personal information to a third-party service provider shall enter into a contract with the third-party that."

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.

## ACLI Comments:

- In order to maintain consistency in terminology throughout the draft, it would be helpful for the term “third party service provider” to be used instead of “third party” or “third-party.” Keeping terminology aligned with the Definitions Section will promote uniformity and cohesive understanding across stakeholders. Additionally, consistency amongst “third party service provider” versus the hyphenated “third-party service provider” would aid in this effort.<sup>1</sup>
- Because licensees might not have the bargaining position to meet all of the requirements under the Chair’s Draft Section 5(A), it is important to include language that accommodates this understanding. Focus on the specific relationship or services provided by the third party service provider pursuant to the agreement, rather than all services that the third party service provider *could* provide, is the most appropriate way to assess and mitigate risk combined with contractual protections.

## ACLI Recommended Revision:

- (A) Contract Requirements. Consistent with the ~~size and complexity of the third-party~~, size, complexity, and risk of the relationship with the third party service provider, a licensee that discloses a consumer’s nonpublic personal information to a third-party service provider shall include contract terms enter into a contract with the third-party that:

### Article II Section 5(A)(1)

**Chair Draft Language:** “(1) Prohibits the third-party from processing the nonpublic personal information for any purpose other than those related to providing the services specified in the contract with the licensee, unless retention is necessary to comply with the law or valid and binding order or a governmental body;”

## ACLI Comment:

- The inclusion of consistent language throughout the Section is essential and important to create a shared understanding of meaning. Because the first clause of Section 5(A)(1) addresses processing, the second clause should address processing as opposed to retention.

## ACLI Recommended Revision:

- (1) Prohibits the third-party from processing the nonpublic personal information for any purpose other than those related to providing the services specified in the contract with the licensee, unless ~~retention~~ processing is necessary to comply with the law or valid and binding order or a governmental body;

---

<sup>1</sup> As opposed to offering red lines throughout the suggested language in this comment letter, we would recommend addressing this consistency in Section 5 and elsewhere where “third party” or “third-party” are used.

## Article II Section 5(A)(4)

**Chair Draft Language:** “(4) Obligates the third-party to enter into written agreements with subcontractors that include provisions requiring them to meet the obligations of the third-party service provider with respect to personal information and provide copies of those contracts to the licensee;”

ACLI Comments:

- The last clause, “provide copies of those contracts to the licensee,” is unfeasible, unworkable, and will not provide any meaningful protection to consumers. Third party service providers are often bound by confidentiality requirements with their own subcontractors such that their provision of these contracts would not be possible. Importantly, issues with the confidentiality of contracts would lead to a severe imbalance in contract negotiating power, forcing companies to do business with only small providers, leaving out important and secure large providers such as AWS, Microsoft, or Google. Some of these third party service providers are crucial to consumer protections such as vendors that support the licensee’s information security programs. Furthermore, this would disadvantage small licensees more significantly as they will have even less leverage.
- If the intention of this last clause is to impose best practices or due diligence on licensees, this is not the vehicle to do so. This requirement is a mandate on the licensee, not necessarily a mandate on the third party service providers. Furthermore, many companies already include due diligence questionnaires which inquire into the third party service provider passing any provisions associated with the protection and use of confidential and sensitive data on to the sub-contractors. Adding in this proposed provision would significantly hinder bargaining power, unfairly disadvantage small licensees, implicate licensees in agreements they are not a party to, and would not serve to protect consumer information any more so than if the copy of the contract was not received and retained by the licensee. Due to these issues, the latter clause should be stricken.

ACLI Recommended Revision:

- (4) Obligates the third-party to enter into written agreements with subcontractors that include provisions requiring them to meet the obligations of the third-party service provider with respect to personal information ~~and provide copies of those contracts to the licensee;~~

## Article II Section 5(A)(6)

**Chair Draft Language:** “(6) Obligates the third-party to implement and maintain reasonable administrative, technical, and physical data security practices to protect the personal data from unauthorized access, destruction, use, modification, or disclosure, and require notification to the licensee of a breach of this term within 48 hours.”

ACLI Comments:

- ACLI does not believe this provision is appropriate or necessary in a Privacy Model because it will duplicate Security Model # 668, duplicate state AG breach notification considerations (to notify the Data Owner), and would trigger an avalanche of negotiations and re-opening of contracts with many third party service providers. Section 5(A)(6) conflates privacy and security which could lead to confusion in state adoption.
- Moreover, this provision conflicts with many state laws and regulations. Specifically, the 48 hour requirement conflicts with the 72 hours required by the NYDFS cybersecurity regulation and the new SEC cybersecurity rule. In fact, the SEC also considered 48 hours but ultimately concluded that time frame was inconsistent with other regulations.
- Lastly, the obligation to notify here is not tied to a breach of nonpublic information; rather, notice is triggered without a breach of nonpublic personal information if the third party service provider fails to implement reasonable controls to protect personal data. If a third party service provider is required to notify customers each time there is a lapse in its security (absent a suspected or actual breach of nonpublic information), consumers would be inundated with notices that are not actionable in any real way. Because this provision is unworkable, conflicts with other established provisions, and conflates privacy and security, we recommend striking the provision in its entirety.

ACLI Recommended Revision:

- ACLI recommends that Article II Section 5(A)(6) be deleted in its entirety.

### Article II Section 5(B)

**Chair Draft Language:** “(B) The licensee is solely responsible for the administration of its data integrity and compliance with this Act and the handling of nonpublic personal information.”

ACLI Comments:

- The last provision in Section 5 would make licensees solely responsible for third party service provider compliance, creating indemnification issues and contract issues. This provision would severely impact allocation of risks and could result in even those who intentionally disregard contractual promises avoiding responsibility for their actions and, where applicable, their own independent legal obligations. Shielding third party service providers who fail to live up to their contractual promises from accountability will actually reduce consumer protection and is out of sync with other privacy enactments.
- Additionally, “data integrity” is not a privacy term that relates to how data is used, but more of a data governance or cybersecurity term that relates to ensuring data is accurate over its lifecycle. This undefined term could be read as creating an additional requirement to the provisions described above. Because this provision allocates responsibility in an unproductive way which could encourage irresponsibility on the part of the third party service provider and utilizes an undefined term, we recommend striking this provision entirely.

ACLI Recommended Revision:

- ACLI recommends that Article II Section 5(B) be deleted in its entirety.

Thank you for the opportunity to share these comments on the Chair's Draft Section 5 Third Party Arrangements. We appreciate that the Chair's Draft generally aligns with developing principles on treatment of third party service provider arrangements adopted in other frameworks including privacy laws in California, Virginia, Utah, Colorado, and Oregon. We believe this consistency with existing frameworks will result in both increased cohesion and likelihood of widespread adoption. We look forward to continued collaboration on this matter and are happy to answer any questions pertaining to the above recommendations.

Thank you,

A handwritten signature in black ink that reads "Kirsten Wolford". The signature is written in a cursive, flowing style.

Kirsten Wolford  
Counsel, Privacy and Cybersecurity  
ACLI  
[kirstenwolford@acli.com](mailto:kirstenwolford@acli.com)  
(202) 624-2059

September 18, 2024

Commissioner Amy Beard, Privacy Protections Working Group Chair  
Erica Weyhenmeyer, Privacy Protections Working Group Vice Chair  
The NAIC Privacy Protections Working Group

Submitted via email: Privacy Protections Working Group: [privacywg@naic.org](mailto:privacywg@naic.org)  
Lois Alexander: [lalexander@naic.org](mailto:lalexander@naic.org)

Thank you for the opportunity to comment on the NAIC Privacy Protections (H) Working Group’s *Article II, Section 5 Third-Party Arrangements*. Health plans have long-been leaders in developing privacy, confidentiality, and cybersecurity practices to protect personal health information. As new technologies emerge and the health care system continues to evolve, AHIP and our members continue to reaffirm our commitment to enhancing patients’ access to actionable information while keeping their personal data secure. At the outset, AHIP would like to strongly state our appreciation in preserving in this draft Model an exemption for Health Insurance Portability and Accountability Act (HIPAA) covered entities. This reflects a continued recognition of the commitment to prioritizing robust protections for patients and their health information.

Below, please find a high-level overview of AHIP’s comments on Article II, Section 5, including questions and recommendations that we respectfully request be considered and discussed during the upcoming September 30 Drafting Group meeting call. For ease of review, AHIP’s questions and recommendations follow the draft / exposed language of Article II, Section 5 Third-Party Arrangements.

AHIP supports policies structured to promote consistency in protections for consumers and alignment across HIPAA covered entities and non-covered entities and applications that collect, use, store, or disclose consumer health information. Where applicable, terms should align with recognized terms under HIPAA as the federal health privacy framework or other industry-utilized federal standards such as those developed by the National Institute for Standards and Technology (NIST). NIST frameworks are developed with significant engagement from stakeholders, including health plans, to ensure applicability across sectors.

**AHIP General Comments / Recommendations:**

- AHIP strongly supports preserving in this draft Model an exemption for HIPAA covered entities.
- Recommend aligning Article II, Section 5 with the language included in HIPAA Business Associate Agreement (“BAA”) provisions relative to third-party’s engagement with subcontractors.
- Recommend the following technical change: consistent use of defined “third-party service provider” throughout the section.

## **ARTICLE II. THIRD PARTY CONTRACUAL OBLIGATIONS**

### **Section 5. Third Party Arrangements**

**A. Contract Requirements. Consistent with the size and complexity of the third-party, a licensee that discloses a consumer’s nonpublic personal information to a third-party service provider shall enter into a contract with the third-party that:**

#### **AHIP Questions / Recommendations for Discussion:**

1. The terms utilized should be consistent with risk-tiering approaches utilized in national standards, such as the [NIST Cybersecurity Framework](#).
2. Recommend including after “third party,” “and the volume and sensitivity of the nonpublic personal information shared”.

**AHIP Item for Future Discussion:** For discussion when the NAIC Privacy Protections (H) Working Group opens Article I, Section 4 “Definition” section, AHIP would like to discuss the definition of “nonpublic personal information”, recommending that the definition of “nonpublic personal information” align with the definition of “personally identifiable information” used by the Office of Management and Budget ([OMB M-17-12](#); [OMB Circular A-130](#)).

**(1) Prohibits the third-party from processing the nonpublic personal information for any purpose other than those related to providing the services specified in the contract with the licensee unless retention is necessary to comply with the law or valid and binding order or a governmental body.**

#### **AHIP Questions / Recommendations for Discussion:**

1. Recommend aligning with HIPAA relative to limited flexibility of permissible activities. For example, HIPAA has exceptions to allow processing of information for certain activities beyond “services” under the Agreement.
2. Recommend the following technical correction: “is necessary to comply with the law or a valid and binding order of a governmental body.”

**(2) Obligates the third party at the licensee’s direction, to delete or return all nonpublic personal information to the licensee when requested; or to delete personal information after it is no longer necessary to fulfill a legal requirement.**

#### **AHIP Recommendations for Discussion:**

1. Recommend aligning with HIPAA, allowing for retention where necessary for the recipient’s proper management and administration or compliance with their legal responsibilities, subject to the limitation that the retained data may be used and disclosed only for such purposes and that the contractual limitations continue to apply.



- Aligning language with HIPAA BAA: Obligates the third party at the licensee’s direction, to delete, return, or continue to protect all nonpublic personal information to the licensee.
2. Recommend the following technical correction: the second line, “personal information” should be changed to “nonpublic personal information.”

**(3) Obligates the third-party to notify the licensee if it can no longer comply with its obligations under this agreement and provides the licensee with a right to terminate the agreement in such case.**

**AHIP Recommendations for Discussion:**

1. Recommend considering adding the following language “or right to terminate if third party fails to cure within a reasonable time period”

**(4) Obligates the third-party to enter into written agreements with subcontractors that include provisions requiring them to meet the obligations of the third-party service provider with respect to personal information and provide copies of those contracts to the licensee.**

**AHIP Questions / Recommendations for Discussion:**

1. Recommend clarifying the responsibility to those third-party service provider downstream entities that are relevant to the activities that the licensee is using.
2. Recommend eliminating the language requiring third-party service providers to provide copies of subcontracts. The scope of vendor diligence must be tailored to the level of risk. We strongly recommend eliminating this language.

**(5) Obligates the third party to provide reasonable assistance to the licensee in fulfilling obligations to respond to consumer requests under Article III of this Act.**

**(6) Obligates the third-party to implement and maintain reasonable administrative, technical, and physical data security practices to protect the personal data from unauthorized access, destruction, use, modification, or disclosure, and require notification to the licensee of a breach of this term within 48 hours.**

**AHIP Recommendations for Discussion:**

1. Recommend deferring to existing laws and practices. Rather than inserting an hour requirement, recommend referencing that the terms with third party service providers for notification of a breach of personal information comply with any applicable laws. HIPAA and states have their own data breach notification requirements.

**B. The licensee is solely responsible for the administration of its data integrity and compliance with this Act and the handling of nonpublic personal information.**

**AHIP Questions / Recommendations for Discussion:**

1. Provide further clarification on the term “data integrity” and discuss third party compliance with the above sections and a licensee being “solely responsible” to the regulator.
2. Under HIPAA, OCR clarified the circumstances under which as a matter of law a covered entity would, and would not, be responsible for the acts and omissions of their BA. How does that compare to the expectations of the NAIC?
3. Recommend deleting this provision in favor of common law principles of principal / agent.

Thank you again for the opportunity to submit comments on the NAIC Privacy Protections (H) Working Group’s *Article II, Section 5 Third-Party Arrangements*. AHIP looks forward to the opportunity to discuss these questions and recommendations during the upcoming September 30 Drafting Group meeting call. Please reach out if you have any questions.

Miranda Motter  
Senior Vice President of State Affairs and Policy  
AHIP  
[mmotter@ahip.org](mailto:mmotter@ahip.org)  
202.923.7346



**Date:** September 18, 2024

**To:** NAIC Privacy Protections Working Group

**From:** American Land Title Association (ALTA)

**Re:** Comments on Updated Draft Model 672 – Section 5

The American Land Title Association (ALTA), representing the real estate settlement services, abstract, and title insurance industry, appreciates the opportunity to provide comments on the most recent draft of proposed Model 672 Article II, Section 5. Facilitation of real estate transfers and financing depends on the title industry's and others' ability to access and communicate transactional information, with significant impacts for the broader economic market. In fact, [a recent economic impact study by EY](#) showed the title industry supports \$82 billion in GDP annually. Given the unique nuances of title insurance work, we value opportunities to provide additional feedback as you seek comments on other sections of Model 672 in the future. Specifically, we will be providing background on the importance of express exemption of publicly available information from this model, which includes public land records which must be accessed and reviewed anytime real estate is transferred or financed.

We identified several Section 5 items that we felt warranted our feedback and have outlined our comments and suggested edits below.

### **Small Business Exemptions**

First and foremost is the cost and practical implementation of compliance for small business licensees. 90% of the title industry is comprised of small insurance businesses. Recognizing the challenges and costs associated with implementation of comprehensive data privacy regimes, states with comprehensive data privacy laws have included some level of small business exemption. Certain states have offered a complete carve-out from compliance for small businesses, while others have provided more limited carve-outs from more costly or resource-intensive requirements. At a minimum, a carve out of certain requirements based on a combination of criteria including annual revenue or yearly total of personal data processed should be provided in the model. This would bring the draft more in line with existing state privacy laws and would reduce the burden on small licensees who may face difficulty – or

impossibility - in implementation based on their limited resources and limited negotiating power in comparison to larger insurance organizations. Because small businesses have less leverage during contract negotiations with third party vendors than larger corporations, a small licensee could face significant added costs of compliance if it means having to renegotiate contracts with a limited pool of vendors willing to meet statutory requirements.

#### **Harmonization with Existing Privacy and Security Laws**

Second, under Section 5(A) specifically, we are concerned that contract requirements are more prescriptive than, and in some cases potentially inconsistent with, the risk-based obligations licensees currently have under the NAIC's model data security law MDL-668 and the requirements in existing state privacy laws. Further, to achieve compliance with the 20 comprehensive state data privacy laws that have been enacted, the California Consumer Privacy Act third-party service provider terms have commonly become the standard. An inconsistency with these terms within Model 672 would mean licensees that have followed this standard would have to renegotiate their third-party vendor contracts, creating additional costs with limited or no added benefit. A better approach would be for the model to allow for existing contracts that contain the terms mandated by the NAIC model data security law, CCPA, or other common regulatory framework to be deemed in compliance with this model.

#### **Implementation Timeframe**

Finally, we suggest allocating a significant period, such as 2 or more years, for licensees to comply with Section 5, knowing there will likely be significant time and cost required for compliant implementation.

Thank you again for the opportunity to provide comments. Should you have any questions regarding this feedback, please contact Elizabeth Blosser at [eblosser@alta.org](mailto:eblosser@alta.org).

September 18, 2024

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) and [privacywg@naic.org](mailto:privacywg@naic.org)

Dear Chair Beard, Vice Chair Weyhenmeyer, and Members of the Privacy Protections Working Group:

Thank you for this opportunity to provide comments on the Privacy Protections Working Group's Chair Draft revising the Privacy of Consumer Financial and Health Information Regulation (#672). APCA<sup>1</sup> appreciates the time, energy, and consideration undertaken by the Privacy Protections Working Group. We value the Working Group's thoughtful approach, ensuring all voices are heard and considered throughout this process.

As requested by the Working Group, these comments primarily relate to Chair Draft Article II, Section 5 – Third Party Arrangements. We also highlight a few provisions related to Third Party Arrangements that require further discussion before drafting is complete. In addition to these comments, we hope you find the attached redline edits constructive and helpful. Please be assured that for each suggestion we are thoughtfully considering how best to balance the intent of the Working Group with legitimate business practices.

While APCA has worked in good faith to identify potential issues and offer constructive suggestions, our comments on third party service providers, and related sections of the Chair Draft, may change as the intent behind certain provisions becomes clearer and the draft continues to take shape. As the Chair Draft evolves, we request sufficient time to revisit this topic, including how third party service providers may affect related sections of the Chair Draft.

---

<sup>1</sup> The American Property Casualty Insurance Association (APCIA) is the primary national trade association for home, auto, and business insurers. APCA promotes and protects the viability of private competition for the benefit of consumers and insurers, with a legacy dating back 150 years. APCA represents the broadest cross-section of home, auto, and business insurers of any national trade association. APCA membership consists of over 1,200 member companies (or over 300 member groups). APCA member companies P&C countrywide market share is 65% (total 73% commercial lines, 55% personal lines).

## Article II, Section 5 Third Party Arrangements

### Section A

The contract requirements of the Third Party Arrangements section should reflect the risk of engagement, and not just the size and complexity of the third party. As shown in the attached redline, APCIA recommends including after “the size and complexity of the third party” the language [“the nature and scope of the third party’s activities, the third party’s relationship with the licensee, and the type of information collected and processed by the third party.”](#)

#### Section A (1)

APCIA members expressed concern with the language in Section A(1) that would “prohibit the third-party from processing the nonpublic personal information for any purpose other than those related to providing the services specified in the contract with the licensee, unless retention is necessary to comply with the law or valid and binding order or a government body.” There may be certain situations where processing nonpublic personal information for other purposes is necessary. This includes, among other possibilities, purposes such as fraud reporting, quality assurance, internal reporting, to enhance future product offerings to the licensee, etc. APCIA members are considering recommendations to address this concern and appreciate the opportunity to provide additional feedback as drafting continues. Additionally, as subsection 1 addresses processing, and retention obligations are more related to the concept of deletion addressed in subsection 2, APCIA recommends the last clause be amended as follows: “unless [processing retention](#) is necessary to comply.”

#### Section A (2)

APCIA members expressed concern with the language in Section A(2) relating to deletion and return requirements. There are certain third party service providers who support compliance functions, such as sanctions screening or fraud reporting, where deleting/returning personal information is unworkable. By design, these third party service providers may retain certain information to support anti-fraud or OFAC compliance. As such, APCIA recommends the Working Group clarify the provision with the following amendment: “or to delete personal information after it is no longer necessary to fulfill a legal requirement [of the licensee or third party service provider.](#)”

#### Section A (4)

The obligation for third party service providers to provide copies of their contracts with subcontractors to the licensee is unworkable and largely unattainable. Third parties are unlikely to comply with this requirement, as contracts are confidential and include

proprietary information. There is no legal obligation to compel the third party to respond as the legal requirement falls to the insurer. This section's contractual requirement will also make contract negotiations unnecessarily complicated and potentially contentious. It would disadvantage small licensees who do not have as much bargaining power as larger licensees. And potentially lead to fewer contracts with large third party service providers unwilling to contractually agree to the new requirements. Further, the potentially high number of subcontractor contracts would be unmanageable and would create volumes of information that would be impossible for any meaningful review. Requiring licensees to acquire and maintain these agreements would also create potential security risks and provides no meaningful protection to the consumer. As shown in the attached redline, APCIA recommends this language be removed.

#### *Section A (6)*

Respectfully, this section is redundant and inconsistent with the 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. For example, the "reasonable security practices" language is inconsistent with the similar requirement in section 4(f)(2) of Model Law 668, which could lead to two different legal standards applying to essentially the same situation. The 48 hour requirement is inconsistent with other laws and regulations, such as the NYDFS cybersecurity regulation which applies a 72 hour time frame. Additionally, the language in this section is somewhat unclear. For instance, the language stating "require notification to the licensee of a breach of this term" would only require vendors to notify about a breach if they violate their data security practices. However, data breaches can occur even if data security practices are not violated. Additionally, vendors have specific breach notification obligations as outlined in the state data breach notification laws, for instance. Given these concerns, APCIA recommends deleting Section A(6) in its entirety.

#### *Section B*

As written, this section is very unclear. Is the purpose to ensure that licensees remain solely responsible for all third party service provider compliance? Will licensees be held liable regardless of how egregious the action of the third party is in all situations? Has the Working Group considered whether and how to define "data integrity" in the context of privacy? Without more clarity around the intent of this section, APCIA recommends Section B be removed completely from the Chair Draft. If drafting evolves, we kindly request the opportunity to offer additional recommendations.

## **Additional Considerations**

### *Section 4. Definitions*

APCIA members have several concerns with the definitions of terms found in Section 4, with many of those concerns being interrelated with the provisions of Chair Draft Article II, Section 5 – Third Party Arrangements.

Specifically, the definition of “*Third Party Service Provider*” should be amended to exclude government entities. It would be extremely challenging, if not impossible, for government entities to agree to these mandated contract provisions. APCIA also recommends that the term “third party service provider” be applied consistently throughout the draft to prevent ambiguity and confusion.

More broadly, terms such as *consumer*, *licensee*, and *non-public personal information* need to be reviewed in the context of the full draft language, rather than through the lens of one section. These terms will also need to be checked throughout the draft for consistency. For instance, *Non-Public Personal Information* appears at times to be conflated with other terms like personal information or personal data. Further, undefined terms such as disclose and process, may need to be defined to provide more clarity.

These concerns are not all encompassing, and only represent some of the definitional questions raised while reviewing Article II, Section 5 – Third Party Arrangements. Additional issues impacting definitions throughout the Chair Draft will likely be identified as drafting evolves. As we foresee potentially negative consequences, we ask that definitional concerns be part of a broader conversation in the future. We will be better able to offer recommendations on all definitions after additional drafting is completed.

### *Section 32. Effective Date*

APCIA recognizes that the Working Group will consider potential concerns with Section 32- Effective Date further along in the drafting process. We look forward to offering additional comments at that time. However, we would like to flag specific implementation concerns as they relate to third party service providers and the Third Party Arrangements section of the Chair Draft. The new requirements under consideration will require licensees to revise existing third party practices, systems, policies, and long-standing contracts. Many existing contracts have agreed upon terms for multiple years into the future and would require renegotiation to account for the changes under consideration in the Chair Draft. These renegotiations could take a significant amount of time and/or require licensees to seek out different vendors willing to accommodate the new requirements. APCIA recommends that



the implementation period be gradual and, as it relates to third party arrangements, apply prospectively to new contracts only.

## **Conclusion**

Privacy is an important matter, and an insurance-specific approach must reconcile with the context of the industry, align with the broader landscape for financial institutions nationally, and consider certain state and federal requirements. Any privacy model law ultimately developed by the NAIC must be practical, reasonable, and workable. It must ensure that its provisions are integrated and work well together and achieve the intended objective of protecting consumers while allowing licensees to meet their business obligations.

We appreciate this opportunity to have APCIA and our members' constructive feedback considered and look forward to ongoing and robust dialogue as the drafting process continues.

Please do not hesitate to contact us with questions.

Thank you,

A handwritten signature in cursive script that reads "Kristin Abbott".

Kristin Abbott

*Senior Director and Counsel, Cyber & Privacy*

American Property Casualty Insurance Association

kristin.abbott@apci.org

## APCIA Redline Suggestions

### Definition

“Third party service provider” means a person or entity not otherwise defined as a licensee or affiliate of a licensee, and not a government entity, that:

- (1) Provides services to the licensee; and
- (2) Maintains, process or otherwise is permitted access to nonpublic personal information through its provisions of services to the licensee.

### Third Party Arrangements

- A. Contract Requirements. Consistent with the size and complexity of the ~~third-party~~ third party, the nature and scope of the third party’s activities, the third party’s relationship with the licensee, and the type of information collected and processed by the third party, a licensee that discloses a consumer’s nonpublic personal information to a ~~third-party~~ third party service provider shall enter into a contract with the a ~~third-party~~ third party that:
  - (1) Prohibits the ~~third-party~~ third party service provider from processing the nonpublic personal information for any purpose other than those related to providing the services specified in the contract with the licensee, unless processing retention is necessary to comply with the law or valid and binding order ~~or of~~ a governmental body;
  - (2) Obligates the ~~third-party~~ third party service provider at the licensee’s direction, to delete or return all nonpublic personal information to the licensee when requested; or to delete personal information after it is no longer necessary to fulfill a legal requirement of the licensee or third party service provider;
  - (3) Obligates the ~~third-party~~ third party service provider to notify the licensee if it can no longer comply with its obligations under this agreement and provides the licensee with a right to terminate the agreement in such case
  - (4) Obligates the ~~third-party~~ third party service provider to enter into written agreements with subcontractors that include provisions requiring them to meet the obligations of the ~~third-party~~ third party service provider with respect to personal information ~~and provide copies of those contracts to the licensee;~~

(5) Obligates the ~~third-party~~ [third party service provider](#) to provide reasonable assistance to the licensee in fulfilling obligations to respond to consumer requests under Article III of this Act.

~~(6) Obligates the third-party to implement and maintain reasonable administrative, technical, and physical data security practices to protect the personal data from unauthorized access, destruction, use, modification, or disclosure, and require notification to the licensee of a breach of this term within 48 hours.~~

~~B. The licensee is solely responsible for the administration of its data integrity and compliance with this Act and the handling of nonpublic personal information.~~

**DEPARTMENT OF INSURANCE****Legal Division, Government Law Bureau**

300 Capitol Mall, 17th Floor  
Sacramento, CA 95814

Damon Diederich  
Privacy Officer / Attorney IV  
TEL: 916-492-3567  
FAX: 916-324-1883  
E-Mail: [Damon.Diederich@insurance.ca.gov](mailto:Damon.Diederich@insurance.ca.gov)  
[www.insurance.ca.gov](http://www.insurance.ca.gov)



September 13, 2024

**VIA ELECTRONIC MAIL**

Commissioner Amy L. Beard  
Indiana Department of Insurance  
311 West Washington Street  
Suite 300  
Indianapolis, IN 46204-2287  
*[E-mail address withheld for privacy]*

**SUBJECT:** NAIC Privacy Protections Working Group –  
Request for Comment re: Chair Draft Article II (Third Party Contractual  
Obligations)

Dear Commissioner Beard:

Thank you for the opportunity to comment on issues relating to regulation of Third Party Service Providers and service contracts, as set forth in the Chair Draft document you developed, and subsequently circulated on August 20.

Rather than attempt to word-smith the draft document, this comment letter will provide some high-level concepts for consideration. These are derived from best practices established in sources like HIPAA, GDPR, and regulations implementing the California Consumer Privacy Rights Act. The relevant portions of those laws are included as appendices to this letter.

Please note that the definition of key terms, like “Third Party Service Provider,” will have major impact on the effect of the Act. While the Definitions section of the Chair Draft is not currently under consideration, the Department looks forward to providing input on that section. Additionally, the Department reserves its right to provide additional comments to this section (Article II – Third Party Contractual Obligations), consistent with the changes ultimately adopted to the Definitions section of the Chair Draft.

### **Requirement for Contract**

Any processing of a consumer's information by a Third Party Service Provider ("TPSP") must occur pursuant to a legally-binding agreement between the insurance institution (i.e.: insurer or producer) and the TPSP. This ensures that the insurance institution will have the ability to ensure appropriate use of, and oversight relating to, consumers' personal information.

During prior discussions relating to Model #674, industry commenters repeatedly raised the "tow truck problem" as an impediment to the contract requirement. Briefly stated, the "tow truck problem" relates to the provision of roadside services as a policy benefit. While insurers have preferred contractors for these services, a consumer's disabled vehicle may be located in an area where an insurer doesn't have a contracted roadside assistance vendor.

Arguably, the best solution to the "tow truck problem" is found in CCPRA regulations: 11 CCR §7050(e) provides that, if a business discloses personal information to a third-party without a contract, the disclosure constitutes "sale/sharing" of the consumer's personal information, and the disclosure is subject to the affirmative election of the consumer.<sup>1</sup> By following this approach, insurers would not be required to contract with each party to which information is disclosed, but disclosure absent a contract would only be permitted if the consumer approves of the disclosure.

Other than under the limited circumstances described above, insurance institution disclosure of personal information should only be pursuant to a contract.

### **Contract Terms**

In order to protect the personal information of consumers, contracts between insurance institutions and TPSPs should contain standard minimum terms. While the parties may elect to include additional terms, certain terms are essential to the protection of consumer privacy and must be universal. Insurers should neither be contracting with entities too small to comply with the requirements of the Act, nor with large entities which refuse to comply with the Act. Not only are standardized contract terms essential for the protection of the consumer, they are also invaluable to the regulator. A standard which allows for different contracting terms based on the size and complexity of the TPSP will yield multiple service contract variants and prove impossible for regulators to enforce.

---

<sup>1</sup> Implementation of this concept will depend on how "sale/sharing" and "opt-in/opt-out" are treated in the Model. Arguably, insurance institutions should not be able to sell/share consumer information, because the information is being provided for the underwriting of coverage (as opposed to social media, wherein the product is provided for free, and personal information is used by the company to generate revenue).

A TPSP contract pursuant to the Act should include these minimum terms:

- Nondelegation: An insurance institution cannot delegate to the TPSP its obligation to comply with the requirements of the Act.
- Purpose Specification: Clearly specify the business purpose(s) for which the insurance institution is sharing the personal information with the TPSP, and the work which the TPSP is expected to accomplish on behalf of the insurance institution.
- Use Limitation: Prohibit any use of personal information by the TPSP, other than consistent with the purposes specified in the contract.
  - Prohibit TPSP from using personal information for any commercial purposes, other than as specified in the contract.
  - Prohibit TPSP from using personal information for any business relationships outside of the agreement with the insurance institution.
- Prohibition on Sale/Sharing: Prohibit the TPSP from selling or sharing the consumer's personal information.
- Compliance with Act: Require that the TPSP agree to comply with the terms of the Act, with respect to personal information shared by an insurance institution.
- Assistance: Require that the TPSP provide reasonable assistance to the insurance institution, in responding to consumer requests pursuant to the Act.
  - Require that the TPSP forward to the insurance institution any consumer requests relating to information obtained pursuant to the Act.
- Safeguards: Require that the TPSP enact administrative, technical, and physical safeguards to ensure the confidentiality, integrity, and availability of personal information shared by an insurance institution.
  - Limit access to personal information to only those TPSP personnel who have a business need to access the personal information, pursuant to the contract, and who have agreed to maintain the confidentiality of the information.
- Notice: Require the TPSP provide notice to the insurance institution of any circumstances potentially affecting the confidentiality of personal information, or the ability of the TPSP to continue performance under the contract.
  - Notice to the insurance institution before the TPSP attempts to enter into any subcontracting arrangements involving personal information.
  - Notice to the insurance institution before any personal information is transferred or processed outside of the United States.
  - Notice to the insurance institution of any incidents affecting the confidentiality, integrity, or availability of personal information.
  - Notice to the insurance institution if the TPSP is no longer, or will no longer be able to comply with its obligations under the Act, or the contract. The insurance institution shall have the right to cancel the contract for noncompliance by the TPSP.

- Subcontracting: Any subcontracts involving personal information shall be subject to the same requirements and limitations as contained in the original contract between the TPSP and the insurance institution. The TPSP shall provide the insurance institution with copies of the finalized contract.
- Compliance Audits: The TPSP shall comply with any requests by the insurance institution to audit, or otherwise verify the TPSP's compliance with, the contract and the Act.
- Deletion of Personal Information: Other than as required by law, at the request of the insurance institution, or at end of the contract, the TPSP shall destroy, or return to the insurance institution, any personal information provided under the contract, and provide verification of the same.
- Choice of Law: The contract shall be subject to venue in, and interpretation under the laws of, a jurisdiction within the United States (Possible: exceptions for nations subject to GDPR, or other comprehensive privacy rights laws).

The Department looks forward to discussing these and other concepts with you and the other members of the Drafting Group during the upcoming September 30 call. Please feel free to reach out with any questions or concerns you may have in the meantime.

Sincerely,



Damon Diederich  
Privacy Officer / Attorney IV

CC: Erica Weyhenmeyer, Vice Chair  
Lois Alexander, NAIC  
Jennifer Neuerberg, NAIC  
Shana Oppenheim, NAIC

Attachment: Appendix A - C

# Appendix A



**§ 164.504 Uses and disclosures:  
Organizational requirements.**

(a) *Definitions.* As used in this section:

*Plan administration functions* means administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan and excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor.

*Summary health information* means information, that may be individually identifiable health information, and:

(1) That summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan; and

(2) From which the information described at § 164.514(b)(2)(i) has been deleted, except that the geographic information described in § 164.514(b)(2)(i)(B) need only be aggregated to the level of a five digit zip code.

(b)-(d) [Reserved]

(e)(1) *Standard: Business associate contracts.* (i) The contract or other arrangement required by § 164.502(e)(2) must meet the requirements of paragraph (e)(2), (e)(3), or (e)(5) of this section, as applicable.

(ii) A covered entity is not in compliance with the standards in § 164.502(e) and this paragraph, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable

steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

(iii) A business associate is not in compliance with the standards in § 164.502(e) and this paragraph, if the business associate knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligation under the contract or other arrangement, unless the business associate took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

(2) *Implementation specifications: Business associate contracts.* A contract between the covered entity and a business associate must:

(i) Establish the permitted and required uses and disclosures of protected health information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:

(A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section; and

(B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.

(ii) Provide that the business associate will:

(A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;

(B) Use appropriate safeguards and comply, where applicable, with subpart C of this part with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by its contract;

(C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410;

(D) In accordance with § 164.502(e)(1)(ii), ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information;

(E) Make available protected health information in accordance with § 164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with § 164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;

(H) To the extent the business associate is to carry out a covered entity's obligation under this subpart, comply with the requirements of this subpart that apply to the covered entity in the performance of such obligation.

(I) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and

(J) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

(iii) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

(3) *Implementation specifications: Other arrangements.* (i) If a covered entity and its business associate are both governmental entities:

(A) The covered entity may comply with this paragraph and § 164.314(a)(1), if applicable, by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (e)(2) of this section and § 164.314(a)(2), if applicable.

(B) The covered entity may comply with this paragraph and § 164.314(a)(1), if applicable, if other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the

business associate that accomplish the objectives of paragraph (e)(2) of this section and § 164.314(a)(2), if applicable.

(ii) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate in § 160.103 of this subchapter to a covered entity, such covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this paragraph and § 164.314(a)(1), if applicable, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(2) of this section and § 164.314(a)(1), if applicable, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.

(iii) The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

(iv) A covered entity may comply with this paragraph and § 164.314(a)(1) if the covered entity discloses only a limited data set to a business associate for the business operations function and the covered entity has a data use agreement with the business associate that complies with § 164.514(e)(4) and § 164.314(a)(1), if applicable.

(4) *Implementation specifications: Other requirements for contracts and other arrangements.* (i) The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the protected health

information received by the business associate in its capacity as a business associate to the covered entity, if necessary:

(A) For the proper management and administration of the business associate; or

(B) To carry out the legal responsibilities of the business associate.

(ii) The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the protected health information received by the business associate in its capacity as a business associate for the purposes described in paragraph (e)(4)(i) of this section, if:

(A) The disclosure is required by law; or

(B)(I) The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person; and

(2) The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(5) *Implementation specifications: Business associate contracts with subcontractors.* The requirements of § 164.504(e)(2) through (e)(4) apply to the contract or other arrangement required by § 164.502(e)(1)(ii) between a business associate and a business associate that is a subcontractor in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.

# Appendix B

3. The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.
4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.
5. The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

#### Article 28

#### Processor

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.
2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.
3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:
  - (a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
  - (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
  - (c) takes all measures required pursuant to Article 32;
  - (d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;
  - (e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;
  - (f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;
  - (g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;
  - (h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

#### *Article 29*

### **Processing under the authority of the controller or processor**

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

#### *Article 30*

### **Records of processing activities**

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

- (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- (b) the purposes of the processing;
- (c) a description of the categories of data subjects and of the categories of personal data;

# Appendix C

sharing of their personal information. The business shall comply with section 7004 when obtaining the consumer's consent.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.*

#### **ARTICLE 4. SERVICE PROVIDERS, CONTRACTORS, AND THIRD PARTIES**

##### **§ 7050. Service Providers and Contractors.**

- (a) A service provider or contractor shall not retain, use, or disclose personal information collected pursuant to its written contract with the business except:
  - (1) For the specific business purpose(s) set forth in the written contract between the business and the service provider or contractor that is required by the CCPA and these regulations.
  - (2) To retain and employ another service provider or contractor as a subcontractor, where the subcontractor meets the requirements for a service provider or contractor under the CCPA and these regulations.
  - (3) For internal use by the service provider or contractor to build or improve the quality of the services it is providing to the business, even if this business purpose is not specified in the written contract required by the CCPA and these regulations, provided that the service provider or contractor does not use the personal information to perform services on behalf of another person. Illustrative examples follow.
    - (A) An email marketing service provider can send emails on a business's behalf using the business's customer email list. The service provider could analyze those customers' interactions with the marketing emails to improve its services and offer those improved services to everyone. But the service provider cannot use the original email list to send marketing emails on behalf of another business.
    - (B) A shipping service provider that delivers businesses' products to their customers may use the addresses received from their business clients and their experience delivering to those addresses to identify faulty or incomplete addresses, and thus, improve their delivery services. However, the shipping service provider cannot compile the addresses received from one business to send advertisements on behalf of another business, or compile addresses received from businesses to sell to data brokers.
  - (4) To prevent, detect, or investigate data security incidents or protect against malicious, deceptive, fraudulent or illegal activity, even if this business purpose is not specified in the written contract required by the CCPA and these regulations.

- (5) For the purposes enumerated in Civil Code section 1798.145, subdivisions (a)(1) through (a)(7).
- (b) A service provider or contractor cannot contract with a business to provide cross-context behavioral advertising. Pursuant to Civil Code section 1798.140, subdivision (e)(6), a service provider or contractor may contract with a business to provide advertising and marketing services, but the service provider or contractor shall not combine the personal information of consumers who have opted-out of the sale/sharing that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or collects from its own interaction with consumers. A person who contracts with a business to provide cross-context behavioral advertising is a third party and not a service provider or contractor with respect to cross-context behavioral advertising services. Illustrative examples follow.
- (1) Business S, a clothing company, hires a social media company as a service provider for the purpose of providing Business S's advertisements on the social media company's platform. The social media company can serve Business S by providing non-personalized advertising services on its platform based on aggregated or demographic information (*e.g.*, advertisements to women, 18-30 years old, that live in Los Angeles). However, it cannot use a list of customer email addresses provided by Business S to identify users on the social media company's platform to serve advertisements to them.
- (2) Business T, a company that sells cookware, hires an advertising company as a service provider for the purpose of advertising its services. The advertising agency can serve Business T by providing contextual advertising services, such as placing advertisements for Business T's products on websites that post recipes and other cooking tips.
- (c) If a service provider or contractor receives a request made pursuant to the CCPA directly from the consumer, the service provider or contractor shall either act on behalf of the business in accordance with the business's instructions for responding to the request or inform the consumer that the request cannot be acted upon because the request has been sent to a service provider or contractor.
- (d) A service provider or contractor that is a business shall comply with the CCPA and these regulations with regard to any personal information that it collects, maintains, or sells outside of its role as a service provider or contractor.
- (e) A person who does not have a contract that complies with section 7051, subsection (a), is not a service provider or a contractor under the CCPA. For example, a business's disclosure of personal information to a person who does not have a contract that complies with section 7051, subsection (a), may be considered a sale or sharing of personal information



for which the business must provide the consumer with the right to opt-out of sale/sharing.

- (f) A service provider or a contractor shall comply with the terms of the contract required by the CCPA and these regulations.
- (g) Whether an entity that provides services to a nonbusiness must comply with a consumer's CCPA request depends upon whether the entity is a "business," as defined by Civil Code section 1798.140, subdivision (d).

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.*

### **§ 7051. Contract Requirements for Service Providers and Contractors.**

- (a) The contract required by the CCPA for service providers and contractors shall:
  - (1) Prohibit the service provider or contractor from selling or sharing personal information it collects pursuant to the written contract with the business.
  - (2) Identify the specific business purpose(s) for which the service provider or contractor is processing personal information pursuant to the written contract with the business, and specify that the business is disclosing the personal information to the service provider or contractor only for the limited and specified business purpose(s) set forth within the contract. The business purpose(s) shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific.
  - (3) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it collected pursuant to the written contract with the business for any purpose other than the business purpose(s) specified in the contract or as otherwise permitted by the CCPA and these regulations.
  - (4) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it collected pursuant to the written contract with the business for any commercial purpose other than the business purpose(s) specified in the contract, unless expressly permitted by the CCPA or these regulations.
  - (5) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it collected pursuant to the written contract with the business outside the direct business relationship between the service provider or contractor and the business, unless expressly permitted by the CCPA or these regulations. For example, a service provider or contractor shall be prohibited from combining or updating personal information that it collected pursuant to the written contract with the business with personal information that it received from another

source or collected from its own interaction with the consumer, unless expressly permitted by the CCPA or these regulations.

- (6) Require the service provider or contractor to comply with all applicable sections of the CCPA and these regulations, including—with respect to the personal information that it collected pursuant to the written contract with the business—providing the same level of privacy protection as required of businesses by the CCPA and these regulations. For example, the contract may require the service provider or contractor to cooperate with the business in responding to and complying with consumers' requests made pursuant to the CCPA, and to implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code section 1798.81.5.
  - (7) Grant the business the right to take reasonable and appropriate steps to ensure that the service provider or contractor uses the personal information that it collected pursuant to the written contract with the business in a manner consistent with the business's obligations under the CCPA and these regulations. Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider's system and regular internal or third-party assessments, audits, or other technical and operational testing at least once every 12 months.
  - (8) Require the service provider or contractor to notify the business after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.
  - (9) Grant the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate the service provider or contractor's unauthorized use of personal information. For example, the business may require the service provider or contractor to provide documentation that verifies that they no longer retain or use the personal information of consumers that have made a valid request to delete with the business.
  - (10) Require the service provider or contractor to enable the business to comply with consumer requests made pursuant to the CCPA or require the business to inform the service provider or contractor of any consumer request made pursuant to the CCPA that they must comply with and provide the information necessary for the service provider or contractor to comply with the request.
- (b) A service provider or contractor that subcontracts with another person in providing services to the business for whom it is a service provider or contractor shall have a contract with the subcontractor that complies with the CCPA and these regulations, including subsection (a).
  - (c) Whether a business conducts due diligence of its service providers and contractors factors into whether the business has reason to believe that a service provider or contractor is

using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that never enforces the terms of the contract nor exercises its rights to audit or test the service provider's or contractor's systems might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intends to use the personal information in violation of the CCPA and these regulations at the time the business disclosed the personal information to the service provider or contractor.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.*

### **§ 7052. Third Parties.**

- (a) A third party that does not have a contract that complies with section 7053, subsection (a), shall not collect, use, process, retain, sell, or share the personal information that the business made available to it.
- (b) A third party shall comply with the terms of the contract required by the CCPA and these regulations, which include treating the personal information that the business made available to it in a manner consistent with the business's obligations under the CCPA and these regulations.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.*

### **§ 7053. Contract Requirements for Third Parties.**

- (a) A business that sells or shares a consumer's personal information with a third party shall enter into an agreement with the third party that:
  - (1) Identifies the limited and specified purpose(s) for which the personal information is made available to the third party. The purpose(s) shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific.
  - (2) Specifies that the business is making the personal information available to the third party only for the limited and specified purpose(s) set forth within the contract and requires the third party to use it only for that limited and specified purpose(s).
  - (3) Requires the third party to comply with all applicable sections of the CCPA and these regulations, including—with respect to the personal information that the business makes available to the third party—providing the same level of privacy protection as required of businesses by the CCPA and these regulations. For example, the contract may require the third party to comply with a consumer's request to opt-out of

sale/sharing forwarded to it by a first-party business and to implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code section 1798.81.5.

- (4) Grants the business the right—with respect to the personal information that the business makes available to the third party—to take reasonable and appropriate steps to ensure that the third party uses it in a manner consistent with the business’s obligations under the CCPA and these regulations. For example, the business may require the third party to attest that it treats the personal information the business made available to it in the same manner that the business is obligated to treat it under the CCPA and these regulations.
  - (5) Grants the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information made available to the third party. For example, the business may require the third party to provide documentation that verifies that it no longer retains or uses the personal information of consumers who have had their requests to opt-out of sale/sharing forwarded to it by the first party business.
  - (6) Requires the third party to notify the business after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.
- (b) Whether a business conducts due diligence of the third party factors into whether the business has reason to believe that the third party is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that never enforces the terms of the contract might not be able to rely on the defense that it did not have reason to believe that the third party intends to use the personal information in violation of the CCPA and these regulations at the time the business disclosed the personal information to the third party.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.*

## **ARTICLE 5. VERIFICATION OF REQUESTS**

### **§ 7060. General Rules Regarding Verification.**

- (a) A business shall establish, document, and comply with a reasonable method for verifying that the person making a request to delete, request to correct, or request to know is the consumer about whom the business has collected information.

September 18, 2024

Chair Amy L. Beard (IN)  
Vice Chair Erica Weyhenmeyer (IL)  
2024 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: Chair's Draft Revising Model Law 672 - Section 5 on Third-Party Arrangements**

Dear Chair Beard and Vice Chair Weyhenmeyer:

The Committee of Annuity Insurers (CAI or Committee)<sup>1</sup> appreciates the opportunity to submit the following comments to the 2024 NAIC Privacy Protections (H) Working Group (Working Group) on the Chair's Draft revising Model 672 (the Chair's Draft). We applaud the Working Group's renewed work on this important issue and its commitment to continuing to work collaboratively over the coming months with consumer and industry stakeholders to craft effective and pragmatic enhancements to consumer privacy protections that are tailored to the insurance sector.

**OVERVIEW**

The CAI recognizes and appreciates the Working Group's efforts to reframe and center the Working Group's efforts around a revised version of Model 672. The Chair's Draft represents a strong basis for enhancing privacy protections for consumers based on an established and time-tested framework that is insurance specific. While there remains a range of important and complex issues to work through in the Chair's Draft, we are confident that the current process will ultimately yield a revised privacy model law that significantly enhances consumer privacy protections while being workable and pragmatic for licensees.

As requested, our comments below focus on issues raised by Section 5 of the Chair's Draft on third-party arrangements. However, there are also related issues raised by Section 5 that necessarily impact other sections of the Chair's Draft, such as the definitions section. Accordingly, we are also commenting on other sections of the Chair's Draft to the extent relevant to issues raised by Section 5. As the Working Group proceeds through the comment and drafting process, we urge the group to keep an eye toward ensuring the revised draft ultimately works as a whole.

In broad scope, the concepts proposed Section 5 are workable and appropriate to ensure a consumer's nonpublic personal information (NPI) is protected when processed by a licensee's third-party service providers. That said, there are several important issues raised by the proposed language that need to be addressed.

---

<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 32 member companies represent approximately 80% of the annuity business in the United States. More information is available at <https://www.annuity-insurers.org/>.

## COMMENTS

**1. The requirements of Section 5 should be integrated into Section 19 to clarify how Section 5's requirements fit into the existing Model 672 structure and avoid creating unintended duplication, confusion, or consequences within the revised model law.**

Model 672 already contains language addressing the use of third-party service providers, including defining contract requirements. That language was carried over into the Chair's Draft as Section 19, with minimal revisions. As a result, the Chair's Draft currently includes two separate and inconsistent sections defining contracting requirements for using third-party service providers. Additionally, Section 5 does not clearly indicate whether joint marketing agreements required under Section 19 also constitute a "third-party arrangement" subject to the requirements of Section 5. Accordingly, the interaction of Section 5 and Section 19 of the Chair's Draft creates some duplication and confusion around how the Section 5 requirements apply.

These issues should be resolved by integrating the requirements of Section 5 into the existing service provider contracting provisions of Section 19, which would also better preserve the existing structure of Model 672 and help avoid unintended consequences that can arise from structural changes to the existing model.

CAI Recommendation. Current Section 5 should be deleted, and instead integrated into the existing Model 672 language on service provider contracts in Section 19.

**2. The minimum contractual obligations should not require third-party service providers to provide their contracts with subcontractors to the licensee.**

As currently drafted, proposed Section 5.A.(4) would require contracts to obligate service providers to put in place contracts with any subcontractors that include the same privacy obligations applicable to the service provider *and* provide copies of those contracts to the licensee. The requirement for third-party service providers to provide the licensees with copies of their contracts with fourth parties would be very difficult, if not impossible, to comply with in practice and is unnecessary to protect consumer privacy.

In practice, fourth-party subcontractors will be unwilling to allow copies of their contracts with the service providers to be disclosed to licensees, as such contracts inevitably contain sensitive corporate information that is closely protected confidential information. For example, such contracts will include pricing information and deal terms that are rightfully considered confidential by participants in a competitive marketplace. Such contracts would often also include other transactional information that may not be relevant to the particular licensee, since the agreement with the subcontractor may be much broader than the scope of the services provided by the subcontractor to the licensee. Accordingly, the terms and nature of these contracts are generally defined as confidential information within the contract itself, and contractually prohibited from being shared.

Changing that would require amendments not only to the licensee's contracts with its third-party service providers, but also by the service providers to their agreements with subcontractors. In many instances, the subcontractor would likely refuse to accept such revised terms, making it impossible for the subcontractor and the licensee to comply with this requirement. If licensees then only limit themselves and their service providers to using those companies willing to agree to these unusual terms, they may be prevented from using the service providers and subcontractors best suited overall to provide the service. Accordingly, requiring this kind of disclosure would make compliance very difficult or impossible in practice, and should be removed.

Further, this requirement is not necessary to meet the policy goals of the PPWG. Even without having to turn over the underlying contracts, service providers will remain responsible for ensuring that equivalent protections for NPI are passed down to their subcontractors and for overall compliance with

the law. Additionally, the Chair's Draft already includes several provisions limiting the redisclosure and reuse of NPI by third parties carried over from existing Model 672, which further help address this issue.

Note also that Section 5.A.(4) currently uses the undefined term "personal information" instead of the defined term "nonpublic personal information", which appears to be an unintended typo.

CAI Recommendation. Section 5.A.(4) should be revised to remove the requirement to provide copies of subcontractor contracts as follows:

*(4) Obligates the third-party to enter into written agreements with subcontractors that include provisions requiring them to meet the obligations of the third-party service provider with respect to nonpublic personal information ~~and provide copies of those contracts to the licensee~~;*

### **3. Clarify the breach notification obligations of Section 5.A.(6).**

Proposed Section 5.A.(6) of the Chair's Draft would require that contracts obligate service providers to maintain reasonable data security practices and notify the licensee "of a breach of this term within 48 hours." This language appears intended to require third-party service providers to notify the licensee of data breaches affecting the licensee's NPI or systems used to provide those services, but as drafted this language does not actually require that.

Instead, as currently drafted, the notification only requires notice be provided where there is a breach "of the term" requiring the third-party service provider to "maintain reasonable administrative, technical, and physical data security practices." Accordingly, a data breach or security incident could occur at the service provider without notice being required if reasonable controls were in place. This does not match up with the apparent intent to ensure that licensees are notified of security incidents affecting their consumer's NPI so they can take appropriate action. This language should be clarified to require notification where there is a security incident affecting NPI of the licensee's consumers or systems used to provide services to the licensee. The requirement to report within 48 hours should also be extended to 72 hours to conform with common market practices and similar existing regulatory requirements (e.g. NY DFS, GDPR).

Note also that Section 5.A.(6) currently uses the undefined term "personal data" instead of the defined term "nonpublic personal information", which appears to be an unintended typo.

CAI Recommendation. Section 5.A.(6) should be revised to clarify that notification of security breaches is required as follows:

*(6) Obligates the third-party to implement and maintain reasonable administrative, technical, and physical data security practices to protect ~~the personal data~~ nonpublic personal information from unauthorized access, destruction, use, modification, or disclosure, and require notification to the licensee of a ~~breach of this term security incident affecting the nonpublic personal information of the licensee's consumers or systems used to provide service to the licensee~~ within ~~48~~ 72 hours.*

### **4. Clarify the obligation for licensees to retain responsibility for third-party service providers.**

Section 5.B. of the Chair's Draft appears intended to clarify that licensees retain ultimate responsibility for the protection of their consumer's NPI consistent with the requirements of the model law regardless of engaging a third-party service provider to perform certain functions. We agree with this principle. However, as drafted this provision is unclear because it uses the undefined and ambiguous terms "data integrity" and "handling" of NPI. This language could be read to have several different meanings and should be clarified.

CAI Recommendation. Section 5.B should be revised as follows:

*B. The A licensee that discloses a consumer’s nonpublic personal information to a third-party service provider remains is solely responsible for the ~~administration of its data integrity and compliance with this Act~~ with respect to such nonpublic personal information and the handling of nonpublic personal information.*

**5. Clarify that the new definition of “Nonpublic Personal Information” includes both “Nonpublic Personal Financial Information” and “Nonpublic Personal Health Information”.**

Because the definition of “Nonpublic Personal Information” is foundational to Section 5 and the Chair’s Draft overall, it is important to avoid any ambiguity in the scope of the definition of NPI. Unlike the original definition of NPI under Model 672, the Chair’s Draft does not clearly include the existing defined terms “Nonpublic Personal Financial Information” (NPMFI) and “Nonpublic Personal Health Information” (NPHI) within NPI. This change could be read to define NPI as something different than, and not fully encompassing, these other existing defined terms. While we do not believe that was the intent of these proposed revisions, any ambiguity in the definition of NPI also creates ambiguity in the scope and extent of application of many other provisions of the Chair’s Draft. The definition of NPI should be revised to expressly include NPMFI and NPHI, like the current definition of NPI under Model 672.

*CAI Recommendations.* The definition of Nonpublic Personal Information in Section 4.V. should be revised as follows:

*V. “Nonpublic personal information” means nonpublic personal financial information, nonpublic personal health information, and any other information that is linked or reasonably linkable to an identified or identifiable natural person.*

A corresponding change to Section 4.W. defining “nonpublic personal financial information” should be made as follows:

*“Nonpublic personal financial information” means ~~nonpublic personal information that includes:~~*

**6. Clarify that the exemptions in Section 21 apply to all NPI, not just NPMFI.**

Section 21 of the Chair’s Draft, carried over from Model 672, provides important exemptions from the notice and opt-out requirements where information is disclosed for certain essential purposes, including to protect against fraud, for institutional risk control, to protect against security incidents, for legal compliance purposes, and in connection with a merger or acquisition. While the Chair’s Draft amended all other existing exemption sections to apply to NPI broadly, Section 21 was not amended and only applies to NPMFI. As drafted the exemptions provided under Section 21 would apply only to the subset of NPI that also constitutes NPMFI. If not corrected, it would limit the ability of licensees to use NPI for fraud prevention and other essential purposes.

*CAI Recommendation.* All references to “nonpublic personal financial information” in Section 21 of the Chair’s Draft should be amended to refer to “nonpublic personal information.”

[Remainder of page left intentionally blank.]




We want to express our deep appreciation for the opportunity to comment on these provisions of the Chair's Draft revising Model 672. 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 cursive script that reads "Stephen E. Roth". The signature is written in black ink and is positioned above a horizontal line.

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

9/16/24

**CONSUMER REPRESENTATIVE COMMENTS ON CHAIR DRAFT  
ARTICLE II. THIRD PARTY CONTRACTUAL OBLIGATIONS**

**Section 5. Third Party Arrangements**

A. Contract Requirements. ~~Consistent with the size and complexity of the third-party, a A~~ licensee that discloses a consumer's nonpublic personal information to a third-party service provider shall enter into a **written** contract with the third-party that:

- (1) Prohibits the third-party from processing nonpublic personal information for any purposes other than those related to providing the services specified in the contract with the licensee.
- (2) Obligates the third-party, at the licensee's direction, to delete, **destroy or return de-identify** all nonpublic personal information when requested, after it is no longer necessary to fulfill a legal requirement, **or after the contract ends**, unless retention is necessary to comply with the law or a valid and binding order of a governmental body.
- (3) Obligates the third-party to notify the licensee if it can no longer comply with its obligations under the agreement and provides the licensee a right to terminate the agreement. **In such case, all obligations to protect nonpublic consumer information shall survive termination of the agreement.**
- (4) Obligates a third-party that enters into **written** agreements with subcontractors to have a written contract that includes provisions that require subcontractors to meet the obligations of the third-party service provider with respect to nonpublic personal information; the third party must provide copies of those contracts to the licensee.
- (5) Obligates the third-party to provide **reasonable adequate** assistance to the licensee in fulfilling obligations to respond to consumer requests under Article III of this Act.
- (6) Obligates the third-party to implement and maintain **reasonable adequate** administrative, technical, and physical data security practices to protect nonpublic personal data from unauthorized access, destruction, use, modification, or disclosure, and requires notification to the licensee of a breach of **this term nonpublic personal information** within 48 hours **of learning of such breach**.

(7) Obligates the third-party to notify the licensee of any instance of the third party failing to meet the obligations in Subsections (1)-(6) above. In such case, the licensee must notify affected consumers within 48 hours after learning of such failures.

(8) Explicitly affirms that any consumer whose nonpublic personal information is shared under the contract is an intended third-party beneficiary of the contract.

B. The licensee is solely responsible for the administration of its data integrity and compliance with this Act and the handling of nonpublic personal information.

Notes:

1. Section A: Deleted "Consistent with the size and complexity of the third-party". This language creates enormous ambiguity and an opportunity for mischief and disagreement.
2. Section A: There should be a written contract. An oral contract would not be sufficient.
3. Subsection A.(2): Returning all nonpublic personal information when requested may have been reasonable when personal information just existed in hard copy. Now that most information is digital, it is not sufficient. Replace "return" with "destroy or de-identify".
4. Subsection A.(3): The last sentence added is modeled after the HIPAA requirement that all PHI protections must survive termination of a Business Associate agreement.
5. Subsections A.(5) and A.(6): Debates over what is reasonable are fraught. Replace "reasonable" with "adequate".
6. Addition of Subsections A.(7) and A.(8): The intention of the model act is to protect consumer information. This language simply makes explicit what is implicit from this intention when consumer information has not been protected, a consumer must promptly be told and has legal standing to act.

## **NAIC Consumer Representative Statement On Key Provisions A New NAIC Privacy Protection Model Should Include**

### Collection and Use

Licensees and their third-party service providers should only collect and use a consumer's nonpublic, personal information to process transactions that a consumer requests or to service a consumer's accounts with the licensee. The consumer can revise such consent at any time.

### Information Sharing

Licensees shall not share a consumer's nonpublic, personal information for purposes other than to process transactions a consumer requests or to service consumer accounts, unless the consumer has given prior consent on a form prescribed by the Model Act. Our proposed content for this consent form is given in Appendix A of this document.

### Contracts With Third Parties

Licensees that share nonpublic, personal information with third parties shall have signed written contracts that require such parties to follow the licensees' privacy policies. Such contracts should:

- a) Prohibit third parties from processing nonpublic, consumer information for purposes other than those specified by the contract;
- b) Require the third party to delete or de-identify non-public personal information when it is no longer needed to process transactions requested by a consumer, to service a consumer's accounts, or to fulfill legal obligations described in the Exceptions section below; and
- c) Enumerate these requirements in clear language that third parties can understand without having to refer to other documents.

### Adverse Underwriting Decisions

Consumers who experience an adverse underwriting decision must have the ability to request the reasons for the adverse decision, including what information was used to make that decision. If the consumer believes that information is incorrect, the consumer should be given the opportunity to correct it and have it submitted for another underwriting review.

## Marketing and Research Studies

Any nonpublic, personal information shall only be used to conduct marketing or research studies and activities if the following conditions are met:

- a) No consumer may be personally identified in any study or report;
- b) A consumer's personal information must be deleted as soon as the information is no longer needed for the specific study or activity; and
- c) The entity conducting the study or activity must agree not to share nonpublic, personal information collected for marketing or research purposes unless the information is de-identified and aggregated.

## Retention and Deletion

Personal information should be deleted or de-identified when it is no longer needed to process transactions requested by a consumer, to service a consumer's accounts, or to fulfill legal obligations described in the Exceptions section below. [A presentation by Eric Ellsworth at the National Meeting in Chicago will address the issue of legacy systems.]

## Exceptions

No section of the Model should restrict activities to prevent criminal activity, fraud, or material consumer misrepresentation or nondisclosure in connection with licensee transactions, as permitted by law.

## Privacy Policy Implementation

Licensees should put in place internal systems and procedures to support implementation of their privacy policies. They should also educate employees about these policies and train employees who have access to consumers' personal information about actions they need to take to ensure these policies are followed.

## Enforcement

For the new privacy model to be effective, there must be sufficient incentive for licensees to comply. Recognizing that it is impractical for state regulators to monitor all licensees for compliance with the Model, state insurance regulators should be given explicit authority to examine and investigate non-compliance concerns. In cases where non-compliance is found, state regulators must be given the ability to impose meaningful administrative actions and in the case of continued non-compliance, meaningful financial penalties.

## APPENDIX A.

### PROPOSED LANGUAGE FOR CONSUMER PRIVACY CONSENT FORMS

We value your privacy and are committed to protecting your personal information. This consent form outlines how we may collect and use your personal information. It also gives you options to specify whether you want to share any of this information for purposes other than to process transactions you request or to service your accounts with us.

#### Information We Collect

We may collect the following categories of personal information:

1. Identifiers: Such as name, email address, Social Security number, passport number, address, contact information
2. Protected Classification Characteristics: Including race, gender, gender identity, age, religion, disability
3. Financial Information: Such as income, assets, past financial transactions, payment history
4. Commercial Information: Such as purchase history, preferences, insurance coverage and claims history
5. Biometric Information: Fingerprints, faceprints, voiceprints
6. Internet or Other Electronic Network Activity Information: Browsing history, search history, interactions with our website
7. Geolocation Data: Physical location or movements
8. Audio, Electronic, Visual, Thermal, Olfactory, or Similar Information: Audio recordings, electronic communications, video recordings
9. Professional or Employment-Related Information: Job history, professional qualifications
10. Education Information: Education information that is not publicly available
11. Inferences Drawn from Other Personal Information: Preferences, characteristics, criminal history, behavior patterns

#### How We Use Your Information

We use your personal information for the following purposes:

- To process your transactions and service your accounts
- To personalize your experience on our website
- To communicate with you about our products, services, and promotions
- To analyze usage trends and preferences
- To comply with legal obligations

## Sharing Your Information

We may share your personal information with the following categories of third parties:

- Service providers who help us operate our business
- Affiliates who offer complementary products or services
- Law enforcement or government agencies when required or permitted by law.

We do not sell your personal information.

## Your Privacy Rights

Under our privacy policy, you have the following rights:

- The right to know what personal information we have collected about you
- The right to request deletion of your personal information
- The right to request correction of incorrect information
- The right to restrict sharing of your personal information
- The right to non-discrimination for exercising your rights.

## Consent to Sharing Of My Personal Information

If you want to let us share certain categories of your personal information for uses other than processing or servicing the insurance transactions you have requested, check the boxes below to indicate which categories of information you are willing to share.

Identifiers (Such as name, email address, Social Security number, passport number, address, contact information)

Protected Classification Characteristics (Including race, gender, gender identity, age, religion, disability)

Financial Information (Such as income, assets, financial transactions, payment history)

Commercial Information (Such as purchase history, preferences, insurance coverage and claims history)

Biometric Information (Fingerprints, faceprints, voiceprints)

Internet or Other Electronic Network Activity Information (Browsing history, search history, interactions)

Geolocation Data (Physical location or movements)

Audio, Electronic, Visual, Thermal, Olfactory, or Similar Information (Audio recordings, electronic communications, video recordings)

Professional or Employment-Related Information (Job history, professional qualifications)

Education Information (Education information that is not publicly available)

Inferences Drawn from Other Personal Information (Preferences, characteristics, criminal history, behavior patterns).

By completing this form, you acknowledge that you have read and understand it.

If you have any questions about your rights under this policy, please contact us at [email address, toll-free phone number, or mailing address].



**From:** [Alexander, Lois](#)  
**To:** [Smid, Rebecca](#)  
**Bcc:** [Beard, Amy](#); [Weyhenmeyer, Erica](#); [Hastings, Victoria](#); [Neuberburg, Jennifer](#); [Weatherford, Holly](#)  
**Subject:** RE: FW: Privacy Protections (H) Working Group - Notice of Public Exposure of Chair Draft Accompanied by Drafting Group Guidelines  
**Date:** Friday, August 23, 2024 10:43:00 AM  
**Attachments:** [jmaae007.png](#)  
[jmaae003.png](#)  
[jmaae004.png](#)  
[jmaae005.png](#)  
[jmaae006.png](#)

Hi Rebecca,

Thank you for your comments. I am sending them to the chairs for the drafting group and will post them following the Sept. 18 deadline.

Lois

**Lois Alexander**  
Manager II – Market Regulation  
Regulatory Services  
O: 816-783-8517  
M: 913-244-9484  
W: [www.naic.org](http://www.naic.org)

**From:** Smid, Rebecca <[Rebecca.Smid@fioir.com](mailto:Rebecca.Smid@fioir.com)>  
**Sent:** Thursday, August 22, 2024 12:27 PM  
**To:** Alexander, Lois <[LAlexander@naic.org](mailto:LAlexander@naic.org)>  
**Subject:** FW: Privacy Protections (H) Working Group - Notice of Public Exposure of Chair Draft Accompanied by Drafting Group Guidelines

**CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.**

Hi Lois,

I suggest removal of the word "reasonable" from number 5 and 6 below. "Reasonable" is too subjective.

A. Contract Requirements. Consistent with the size and complexity of the third-party, a licensee that discloses a consumer's nonpublic personal information to a third-party service provider shall enter into a contract with the third-party that:

- (1) Prohibits the third-party from processing the nonpublic personal information for any purpose other than those related to providing the services specified in the contract with the licensee, unless retention is necessary to comply with the law or valid and binding order or a governmental body;
- (2) Obligates the third-party at the licensee's direction, to delete or return all nonpublic personal information to the licensee when requested; or to delete personal information after it is no longer necessary to fulfill a legal requirement;
- (3) Obligates the third-party to notify the licensee if it can no longer comply with its obligations under this agreement and provides the licensee with a right to terminate the agreement in such case;
- (4) Obligates the third-party to enter into written agreements with subcontractors that include provisions requiring them to meet the obligations of the third-party service provider with respect to personal information and provide copies of those contracts to the licensee;
- (5) Obligates the third-party to provide reasonable assistance to the licensee in fulfilling obligations to respond to consumer requests under Article III of this Act.
- (6) Obligates the third-party to implement and maintain reasonable administrative, technical, and physical data security practices to protect the personal data from unauthorized access, destruction, use, modification, or disclosure, and require notification to the licensee of a breach of this term within 48 hours.



**Rebecca Smid**  
Director of Market Research and  
Technology  
[Rebecca.Smid@fioir.com](mailto:Rebecca.Smid@fioir.com)  
Office: (850) 413-5021

**Florida Office of  
Insurance Regulation**  
200 East Gaines Street,  
Tallahassee, FL 32399  
[www.FLQIR.com](http://www.FLQIR.com)

**From:** Alexander, Lois <[LAlexander@naic.org](mailto:LAlexander@naic.org)>  
**Sent:** Tuesday, August 20, 2024 6:33 PM  
**To:** Alexander, Lois <[LAlexander@naic.org](mailto:LAlexander@naic.org)>  
**Subject:** Privacy Protections (H) Working Group - Notice of Public Exposure of Chair Draft Accompanied by Drafting Group Guidelines

[External Email](#)

**TO THE PRIVACY PROTECTIONS (H) WORKING GROUP (PPWG), WORKING GROUP MEMBERS, INTERESTED REGULATORS, AND INTERESTED PARTIES:**

**PUBLIC NOTICE: THE CHAIR DRAFT REVISING THE PRIVACY OF CONSUMER FINANCIAL AND HEALTH INFORMATION REGULATION (#672) IS BEING EXPOSED FOR A 30-DAY PUBLIC COMMENT PERIOD. WE ARE REQUESTING COMMENTS ON ARTICLE II, SECTION 5 THIRD-PARTY ARRANGEMENTS ONLY. GUIDELINES FOR DRAFTING GROUP MEMBERSHIP AND PARTICIPATION ARE ALSO INCLUDED IN THIS EMAIL.**

**CHAIR DRAFT PUBLIC EXPOSURE**

As discussed during our open meeting at the NAIC Summer National Meeting in Chicago, the Chair Draft revising Model #672 is hereby released for a 30-day public comment period specific to *Article II, Section 5 Third-Party Arrangements*. Comments on other sections of the Model will be requested during later exposure periods. A copy of the exposed Chair Draft is attached to this email and will be posted in the Exposure

Drafts section on the [Privacy Protections \(H\) Working Group webpage](#).

**Written comments on Section 5 - Third-Party Arrangements will be accepted through Wednesday, September 18, 2024, by close of business and should be submitted to Lois Alexander ([lalexander@naic.org](mailto:lalexander@naic.org)).**

**DRAFTING GROUP MEMBERSHIP AND PARTICIPATION GUIDELINES**

The Drafting Group will be led by PPWG Vice-Chair Erica Weyhenmeyer and will be open to working group members and interested parties. The Guidelines for Drafting Group Participation provides information on membership and participation. The Guidelines will be posted to the Documents section of the [PPWG webpage](#).

For interested parties, membership will be limited as detailed in the Guidelines. Each interested party group should designate at least one primary representative and additional representatives may be selected by the interested party groups on a meeting-by-meeting basis. Please refer to the Guidelines for more information.

**Please send Drafting Group volunteer names, titles, emails, and phone numbers to [lalexander@naic.org](mailto:lalexander@naic.org) by Friday, September 6, 2024**, for consideration by the Chair and Vice Chair. For interested parties, if the Drafting Group receives more volunteer requests than the allotted number of representatives and, if a primary representative is not selected, the Chair and Vice Chair will make the selection.

Thank you and we look forward to hearing from you.

**Lois E. Alexander, CFE, MCM, FLMI, HIA, ACP**  
Manager II – Market Regulation  
Regulatory Services

**O:** 816-783-8517  
**M:** 913-244-9484  
**W:** [www.naic.org](http://www.naic.org)

Follow the NAIC on

-----  
**CONFIDENTIALITY NOTICE**  
-----

This message and any attachments are from the NAIC and are intended only for the addressee. Information contained herein is confidential, and may be privileged or exempt from disclosure pursuant to applicable federal or state law. This message is not intended as a waiver of the confidential, privileged or exempted status of the information transmitted. Unauthorized forwarding, printing, copying, distribution or use of such information is strictly prohibited and may be unlawful. If you are not the addressee, please promptly delete this message and notify the sender of the delivery error by e-mail or by forwarding it to the NAIC Service Desk at [help@naic.org](mailto:help@naic.org).

**External Email:** Please do not click on links or attachments unless you know the content is safe.

September 18, 2024

The Honorable Amy Beard  
Chair  
Privacy Protections Working Group  
National Association of Insurance Commissioners  
1100 Walnut Street, Suite 1000  
Kansas City, MO 64106-2197s

*Re: Chair Draft Comments / Third-Party Service Providers (Section 5)*

Dear Commissioner Beard:

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 perspective regarding the proposed revisions to NAIC Model Law 672 outlined in the Chair Draft.

### **Initial Comments**

IIABA recognizes and appreciates the desire of the NAIC to review its existing privacy-related proposals for state policymakers and to update and upgrade those model law recommendations. It is appropriate for the NAIC to revisit these issues and consider more robust requirements, especially given the magnitude of privacy activity that has occurred in statehouses over the last three-and-a-half years. Privacy is important to our members and the consumers they serve, and we welcome the opportunity to be part of the important public policy discussions that will occur in the weeks to come. Our members utilize the nonpublic personal information of customers to address their insurance needs and share it when necessary to provide products and services to those consumers, and we do not object to reasonable and thoughtfully crafted enhancements in this area.

A geographically and politically diverse group of 20 states, which represent more than half of the population in our country, have now enacted comprehensive privacy laws<sup>1</sup> (with 19 of those jurisdictions passing statutes since the start of 2021). The universe of states adopting similar measures is almost certain to grow in 2025 and beyond. As you consider how to modify and enhance Model 672, we urge you to look to and be mindful of this flurry of public policymaking activity and the resulting body of privacy law that has emerged. Each of these statutes expressly exempts insurance licensees, banks, and other financial institutions from their scope (because of the privacy requirements that already apply to these entities), but these laws are instructive and remain very relevant to the work you will be doing.

---

<sup>1</sup> The following states have enacted comprehensive privacy laws: California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, and Virginia.

Although the comprehensive privacy statutes now in place have often been described as a patchwork of laws, these measures generally include many of the same core elements, address those issues in a similar way, and have produced a fairly consistent regulatory framework. As you consider how to revise and bolster the insurance-specific requirements of Model 672, we urge you not to propose requirements and industry burdens that are dramatically different and harsher than the privacy mandates quickly being established for other industries. A model law that proposes anomalous guidelines and unique standards for any single business sector will face substantive, political, and legal obstacles and is unlikely to be considered seriously by policymakers. This is especially true for the insurance industry, which is already subject to longstanding federal privacy requirements and has been exempted from the recently enacted state privacy laws.

IIABA commends you and Vice Chair Weyhenmeyer for producing an initial draft that provides the working group and stakeholders with a sound and thoughtful starting point for the discussion and refinement that will ensue. The draft builds on the privacy regime that exists today in the insurance world and would add an array of new requirements and restrictions. These new sections address the same privacy-related topics that have been addressed in the comprehensive state privacy statutes, including restrictions on the sale of nonpublic personal information and the use of sensitive personal information, requirements that apply when nonpublic personal information is shared with third-party service providers, and provisions that enable consumers to access their nonpublic personal information and request the correction or deletion of that material.

IIABA also thanks the Chair, Vice Chair, and working group members for developing a sensible work plan for considering the revisions. Tackling these topics on an issue-by-issue basis and then addressing any necessary clean-up and ancillary items makes good sense, and our association looks forward to participating in this process. Some of the issues you will consider are less contentious and likely easier to tackle and finalize. The topics that may be the most challenging to address are arguably the requirements that relate to third-party service providers, and IIABA offers its comments on this subject below.

### **Third Party Contractual Obligations**

#### *Application and Scope*

Section 5 is a proposed new addition to Model 672 that would require any insurance licensee who discloses nonpublic personal information to a third-party service provider to enter into a contract with that entity. The section would require such contracts to include a series of very specific elements. It is not surprising that the working group would consider requirements related to the sharing of nonpublic personal information with service providers, as this is an issue that has been addressed in the comprehensive state privacy laws that have been enacted over the past several years.

IIABA has strong concerns, however, with requiring insurance agencies to dictate the data privacy practices of third-party service providers as outlined in the draft. These proposed requirements would apply to all licensees, including all insurance agencies regardless of size, and the typical insurance agency is in no position to force contractual demands of this nature upon larger and more sophisticated vendors. It is not uncommon for critically important service providers to present contracts to licensees on a take-it-or-leave-it basis and without meaningful opportunity for negotiation, and the draft would establish untenable requirements that cannot be satisfied by main street insurance agents due to marketplace realities.

Notably, the application of these contractual requirements to all insurance licensees is inconsistent with the recently enacted state privacy laws. Those acts do not apply third-party service provider contract mandates to small- and medium-sized businesses. The comprehensive state privacy laws generally apply such requirements to businesses who maintained the nonpublic personal information of a specified number of state consumers in the previous year, and those consumer applicability thresholds range from 35,000 to 175,000 residents. Two other states (Nebraska and Texas) only apply requirements of this nature to businesses who do not qualify as small businesses under regulations promulgated by the federal Small Business Administration. As a result, any NAIC model law that proposes service provider contractual obligations for all insurance licensees (including all agencies) is significantly different and far more expansive and onerous than the privacy regimes already being put in place by state policymakers.

IIABA urges you to address this issue in one of two ways:

- *Direct Application of Requirements to Third-Party Service Providers* – Section 5 is presumably intended to ensure that third-party service providers will act (or not act) in particular ways and engage (or not engage) in certain practices. Rather than instituting such requirements directly, however, the proposal places the burden of policing service providers on licensees and requires licensees to dictate very specific contractual terms to providers. This is challenging and unrealistic for the reasons discussed above. This scenario is additionally troubling because the failure or inability of an insurance agency to convince a service provider to enter into such a contract could prevent that business from securing services that are crucial to meet client needs or result in statutory violations, enforcement actions, and fines. It should also be noted that even if a licensee is able to secure the contractual terms required by the proposal, there is no guarantee that a service provider will actually honor the agreement or any assurance that the anticipated public policy outcomes will be achieved. Service providers could ignore or violate the contract, and the proposal as drafted offers no mechanism for compelling compliance in such an instance.

An alternative and more efficient and effective way to address these subjects would be to impose requirements on third-party service providers directly. The working group could propose the establishment of whatever statutory requirements it chooses for service providers, and state insurance regulators or some other state agency or official (e.g., a state attorney general) could be charged with enforcement of those obligations. This commonsense approach has successful precedents in both federal and state law, and the direct application of such requirements on service providers would be more likely to produce the public policy outcomes you seek.

- *Limited Exemption* – A second option for the working group is to limit the applicability of Section 5 or to include a limited exemption that more closely mirrors the comprehensive state privacy laws. There are numerous ways in which such a provision could be crafted, but one possibility would be to add the following as a new subsection:

\_\_\_ *The requirements of this section shall not apply to a licensee that:*

- (a) Controlled or processed the nonpublic personal information of fewer than 35,000 resident consumers during the preceding calendar year; or*
- (b) Is a small business as defined by the federal Small Business Administration.*

This recommendation follows the example that has been provided by the comprehensive state privacy laws, and the consumer threshold proposed above is the lowest such threshold found in any of those statutes. Adding a limited exemption of this nature will help harmonize the model law with state privacy statutes, avoid an outcome in which the insurance industry is uniquely subjected to harsher privacy requirements, and increase the likelihood that this model will be considered and enacted by state legislators.

We should note that we envision this as a limited exemption (from Section 5 and perhaps additional requirements that may be considered by the working group at a later time) and not a complete exemption from all of the model's requirements.

### *Contractual Elements*

Section 5 would require licensees to compel service providers to enter into contracts when nonpublic personal information is disclosed, and paragraphs (A)(1)-(6) identify the six elements that would be required in such a contract. Several of the items should be revised or deleted altogether because they are unnecessary or because they extend well beyond what is required of businesses under the comprehensive state privacy laws. In general, we urge you to consider whether these required contractual elements are consistent with those laws or whether they impose harsher treatment on the insurance industry. The working group might also consider whether a contract that would satisfy the contract obligations established by the state privacy laws would also satisfy the requirements proposed in the Chair Draft.

As you consider revisions to Section 5(A), we urge you to at least consider the following two items:

- Section 5(A)(4) contemplates licensee-service provider contracts that would require a third-party service provider to provide all of its subcontractor agreements to a licensee. This would be an unprecedented, burdensome, and disruptive requirement and one that does not offer any meaningful public policy benefit. Accordingly, IIABA urges you to delete the contract disclosure requirement from this paragraph.
- IIABA also urges the working group to delete Section 5(A)(6). This paragraph would require licensees to compel service providers to agree to contractual terms related to data security. This provision should be deleted since the subject matter is already addressed in the NAIC's *Insurance Data Security Model Law* and because the requirements of that model (which are now in place in nearly half of the states) differ from what is proposed in the Chair Draft.

### *Subsection (B)*

IIABA and its members are also very concerned by the inclusion of Subsection (B). The purpose and effect of this provision are unclear, and there is no precedent for this unusual item in the comprehensive state privacy laws. We urge the working group to delete the subsection and perhaps replace it with the following text more appropriate for this section:

- B. The Licensee shall exercise due diligence in selecting third-party service providers.*

### *Technical Issues and Other Comments*

There are instances in Section 5 where the term “third party” is used as a substitute for “third-party service provider.” In order to eliminate the possibility of confusion, IIABA recommends that the working group delete the references to “third party” and use the term “third-party service provider” consistently throughout the section, including in the titles for Article II and Section 5. Similarly, the working group should also replace “personal information” with “nonpublic personal information” in Section 5(A)(2) and (4).

The comments we have provided above respond to the August 20 request for input concerning Section 5 of the Chair Draft, but IIABA also looks forward to providing the working group with our thoughts regarding the definition of “nonpublic personal information” at the appropriate time. This definition is used throughout Section 5 and has been (perhaps inadvertently) expanded significantly, and the working group will likely want to consider the effect this much broader definition has on Section 5 and other elements of the proposal. IIABA believes it is critical that the definition of “nonpublic personal information” exclude “publicly available information” from its scope (as is the case with the comprehensive state privacy laws and other privacy frameworks), and we urge the working group to incorporate this and other appropriate revisions into its next draft.

### **Conclusion**

IIABA thanks you and the working group for your consideration of our views and looks forward to working with you as your efforts continue. If we can provide any additional information or assistance, 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,



Wesley Bissett  
Senior Counsel, Government Affairs



*Electronically Submitted to lalexander@naic.org*

September 17, 2024

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

**Re: Exposure Draft of Revisions to the Privacy of Consumer Financial and Health Information Regulation (#672)**

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 Chair Draft Exposure of the Privacy of Consumer Financial and Health Information Regulation (the “Exposure Draft”). We are appreciative of the Working Group’s continued efforts on this important issue. While we anticipate that our members will have comments on the other sections of the draft, per the Working Group’s request, we are only providing comments at this time on **Article II, Section 5, Third-Party Arrangements**. Our comments and recommendations are outlined as follows:

1) **Section 5(A)(1)**: Since this provision is intended to address “processing” of nonpublic personal information, we recommend the following redline change:

(1) Prohibits the third-party from processing the nonpublic personal information for any purpose other than those related to providing the services specified in the contract with the licensee, unless ~~retention~~ **processing** is necessary to comply with the law or valid and binding order or a governmental body;

2) **Section 5(A)(2)**: Our members have concerns about the practicability of this provision. Many service providers seek to purge personal information in archives/backups in accordance with their typical archive process, as opposed to immediately deleting a customer's information upon termination. Additionally, some service providers require the customer to retrieve and delete information on their systems. Having contractual

---

<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.



terms that would dictate something different than the typical retention practices may not be feasible or practical here, and more flexible language is needed to allow deletion in accordance with documented record retention policies.

**3) Section 5(A)(4):**

- a. The language “to meet the obligations of the third-party service provider” is too broad, and we’d suggest this be limited to the “privacy obligations” of the third-party service provider.
- b. Our members have significant concerns with the language obligating third parties to “provide copies of [subcontractor] contracts to the licensee”, and we recommend that this language be removed. Simply put, service providers are unlikely to contractually agree to provide copies of their subcontractor contracts. In fact, they may have confidentiality obligations that would prohibit them from sharing these contracts. A requirement to collect these contracts also does not provide any additional protections for the consumer. As long as the licensee’s contracts with the third-party service provider contains the appropriate representations and warranties regarding subcontractor contracts, this should be sufficient. As such, requiring third-party service providers to provide copies of all contracts with their subcontractors would have a negative impact on insurers’ ability to do business with certain providers who would not agree with such terms, without providing any actual protection for consumers.

**4) Section 5(A)(6) and 5(B):**

- a. These provisions appear more focused on data security, and it would be more appropriate to address these in a data security model law as opposed to within the privacy requirements. One approach could be to simplify 5(B) by modifying it to read “The licensee is responsible for compliance with this Act.”

Also, we strongly encourage the Working Group to add language making it clear that these new contractual requirements are effective on a “go-forward basis” and are only applicable to new agreements or renewals after a specified date. This language is important to ensure that all existing agreements won’t require immediate renegotiation as soon as the requirements are effective. This would have a negative impact on our members’ ability to continue their normal business and operations. We understand that any implementation and/or effective dates need to be addressed holistically, and the Working Group may plan to address this later, but because of the impact of this on Section 5, we wanted to raise this issue now for consideration.

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)

## Comments on Draft Privacy Model

Bob Wake, Maine Bureau of Insurance

September 18, 2024

**Markup:** I have followed these comments with a markup of the relevant material. I hope that was helpful, but this was only feasible because it was a very short excerpt from the PDF. In the future, it would be extremely helpful to provide commenters with access to a draft in MS-Word format. This is particularly important when working from a document with tracked changes, since copying from a PDF into a Word document removes all distinction between original text, added text, and deleted text.

**Comments on Article I:** These comments are premature if there is a separate comment period for proposed Sections 1 through 3, but I am offering them now in case they were skipped over because they were unchanged from existing language and seemed noncontroversial. Existing Section 1 was deleted because is not appropriate for legislation, and only made sense in the context of a regulation. The “Purpose and Scope” section will need some additional enumerated purposes to be added later, and should not be referring to “personal health information and personal information” as though personal health information were not a type of personal information. I have suggested a few other editorial changes, including clarification of why This State is saying anything at all about licensees’ activities in other states. Finally, if the clause about safe harbor notices was ever appropriately designated as a “rule of construction” and placed in Article I, that treatment is no longer appropriate with the new version of that clause, and its content should be moved down to the section on notices.

**Definition of Third-Party Service Provider:** While the definitions in general are a topic of future comments, it seems as though this definition should be reviewed in tandem with the substantive section establishing TPSPs’ obligations. At this stage, however, my only substantive concern is to ensure that if we define a licensee’s affiliate not to be a TPSP, we need to keep a reminder in the “parking lot” that we will need other provisions ensuring that if nonpublic personal information is shared with an affiliate that is not itself a licensee, there needs to be an effective mechanism obligating the affiliate to provide the same protections that a licensee or TPSP is obligated to provide. I have also made some editorial revisions, including hyphenating “third-party” only when the term is used as an adjective.

**Obligations of TPSPs:** This draft follows the “HIPAA 1.0” approach, under which the obligations of the licensee are created by law and are enforceable by the State, while the obligations of the TPSP are created solely by contract and enforceable only by the licensee. The HIPAA regulations, however, were amended years ago to give business associates legal as well as contractual obligations, and we should consider the same. This would be essential if we were to consider any sort of *de minimis* “tow truck” exemption such as the industry was proposing last year. Hopefully they do not, but if they were to persuade the NAIC that there some situations where it is simply not feasible to require a written contract, there should at the very least be a requirement to warn them that it is illegal to sell or otherwise misuse the nonpublic personal information they have received. This would require making that conduct illegal.

**Proportionality trigger:** Is “consistent with the size and complexity of the third party” the right wording here? Or is it even necessary at all? Other factors that might be relevant are the size and complexity of the licensee (the industry draft dealt with this by limiting the obligation to large companies doing business in large states) and the nature sensitivity of the information being disclosed. But do any of these factors affect the need

**“Processing”:** This isn’t an unreasonable word to use as a catch-all to encompass all the activities we need to restrict, but it’s a technical term that will need a definition.

**“Written contract”:** The draft refers variously to a “contract,” and “agreement,” and a “written agreement.” The use of different terms implies that “contract” and “agreement” might have different meanings, and I see no reason to require subcontracts to be in writing but not the prime contract, so I propose replacing “agreement” with “contract” and requiring a “written contract” at both levels.

**“Breach of this term”:** The draft requires the TPSP to maintain reasonable security procedures and to notify the licensee within 48 hours after any “breach of this term.” As written, the trigger for notice is a breach of contract, *i.e.*, the licensee’s decision to stop maintaining reasonable security procedures. The trigger ought to be a security breach, even if the TPSP has been in compliance with its contractual obligations and was simply unlucky.

**“Solely responsible”:** We want the licensee and the TPSP to be jointly responsible. We don’t want to impose obligations on the TPSP in Paragraph A and then absolve the TPSP in Paragraph B from any responsibility for failure to comply.

## ARTICLE I. GENERAL PROVISIONS

### ~~Section 1.~~— Authority

~~This Act is promulgated pursuant to the authority granted by Sections [insert applicable sections] of the Insurance Law.~~

### Section 21. Purpose and Scope

A. Purpose. This Act governs the treatment of nonpublic personal ~~health information and nonpublic personal information~~ about individuals by all licensees of the state insurance department. This Act:

- (1) Requires a licensee to provide notice to individuals about its privacy policies and practices;
- (2) Describes the conditions under which a licensee may disclose nonpublic personal ~~health information and nonpublic personal~~ information about individuals to affiliates and nonaffiliated third parties; ~~and~~

(3) Provides methods for individuals to prevent a licensee from disclosing that information; and

*(4, etc.) [to be reviewed later].*

B. Scope. This Act applies to:

~~(12) All nonpublic personal health information; and;~~

(1) Nonpublic personal information, other than health information, about individuals who obtain ~~or are claimants or beneficiaries of~~ products or services from licensees primarily for personal, family or household purposes from licensees or are claimants or beneficiaries of such products. This Act does not apply to information about ~~companies business entities~~ or about individuals who obtain products or services for business, commercial or agricultural purposes; ~~and~~

~~(2) All nonpublic personal health information;~~

~~C. Compliance. A licensee domiciled in this state that is in compliance with this Act in a state that has not enacted laws or regulations that meet the requirements of Title V of the Gramm-Leach-Bliley Act (PL 102-106) may nonetheless be deemed to be in compliance with Title V of the Gramm-Leach-Bliley Act in the other state.~~

~~Drafting Note: Subsection C is intended to give licensees some guidance for complying with Title V of the Gramm-Leach-Bliley Act in those states that do not have laws or regulations that meet GLBA's privacy requirements.~~

**Section 3. — Rule of Construction** ~~XXX. [to be moved and retitled].~~

The Commissioner shall provide examples on their website of privacy notices to be used by licensees as a safe harbor for compliance with this Act.

Formatted: Font: Italic

**Section 42. Definitions**

As used in this Act, unless the context requires otherwise:

\*\*\*\*\*

CC. “Third party service provider” means a person or entity that is not otherwise defined as a licensee or affiliate of a licensee ~~that and;~~

(1) Provides services to the licensee; and

(2) Maintains, processes, or otherwise is permitted access to nonpublic personal information through its ~~provisions~~ provision of services to the licensee.

\*\*\*\*\*

Commented [RAW1]: See comment

Commented [RAW2]: ???

Commented [RAW3]: see comment

ARTICLE II. THIRD-PARTY ~~CONTRACUAL-CONTRACTUAL~~ OBLIGATIONS

Commented [RAW4]: see comment

Section 53. Third-Party Arrangements

A. Contract Requirements. Consistent with the size and complexity of the third-party, a licensee that discloses a consumer’s nonpublic personal information to a third-party service provider shall enter into a written contract with the third-party that:

Commented [RAW5]: see comment

Commented [RAW6]: see comment

(1) Prohibits the third-party from processing the nonpublic personal information for any purpose other than those related to providing the services specified in the contract with the licensee, unless retention is except as necessary to comply with the law or valid and binding order or a governmental body, in which case the third party must notify the licensee unless prohibited by law;

Commented [RAW7]: see comment

(2) Obligates the third-party at the licensee’s direction, to delete or return all nonpublic personal information to the licensee when requested; or to delete personal information after it is no longer necessary to fulfill a legal requirement, unless retention is necessary to comply with the law or a valid and binding order of a governmental body;

(3) Obligates the third-party to notify the licensee if it can no longer comply with its obligations under this agreementthe contract and provides the licensee with a right to terminate the agreement-contract in such-that case;

(4) Obligates the third-party, if any subcontractor is granted access to nonpublic personal information, to enter into a written agreementcontracts- with the subcontractor, and to provide a copy of the contract to the licensee,s -that includes provisions requiring them-the subcontractor to meet the obligations of the third-party service provider with respect to personal information-and provide copies of those contracts to the licensee;

(5) Obligates the third-party to provide reasonable assistance to the licensee in fulfilling obligations to respond to consumer requests under Article III of this Act.

(6) Obligates the third-party to implement and maintain reasonable administrative, technical, and physical data security practices to protect the personal data from unauthorized access, destruction, use, modification, or disclosure, and require obligates the third party to notification-ty the licensee of any data breach of this term-within 48 hours.

Commented [RAW8]: see comment

B. The licensee is solely-remains fully responsible for the administration of its data integrity and compliance with this Act and the handling of nonpublic personal information.

Commented [RAW9]: see comment



September 18, 2024

Commissioner Amy L. Beard  
Indiana Department of Insurance  
Chair, NAIC Privacy Protections (H) Working Group  
311 W Washington Street  
Indianapolis, IN 46204

*Sent Via Electronic Mail*

Dear Commissioner Beard,

I am writing on behalf of the National Association of Benefits and Insurance Professionals (NABIP), formerly known as NAHU, an association representing over 100,000 licensed health insurance agents, brokers, general agents, consultants, and employee benefits specialists. Our members are dedicated to providing consumers with comprehensive, fair, and accessible health insurance options. NABIP has adopted a Consumer Healthcare Bill of Rights, which ensures that every individual receives transparent information, privacy protection, and fair treatment when it comes to health insurance and financial security. Specifically, this letter addresses Article IV of NABIP's "Bill of Rights," which focuses on consumer privacy and data security, as we comment on the Chair's Draft Amendments to the NAIC Model #672, "Privacy of Consumer Financial and Health Information Regulation."

NABIP appreciates the Committee's decision to revise the existing model rather than creating an entirely new privacy protections model law, ensuring continuity and clarity for consumers and industry stakeholders.

Our association would also like to express our gratitude for your decision to carry forward a choice made by the Privacy Protections Working Group during its deliberation over last year's draft of the model. Specifically, in Article Seven, Section 21 of the Chair's Draft, the act will not apply to licensees who are already subject to the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) privacy and data security requirements, provided they maintain nonpublic personal information in the same manner as protected health information (PHI). Individuals and entities licensed by state departments of insurance, who are subject to HIPAA and HITECH, have spent the last two decades building systems, policies, and procedures to safeguard PHI and nonpublic personal information. Moreover, consumers are familiar with and trust these protections. Therefore, ensuring that those who comply with HIPAA/HITECH requirements are not subjected to redundant regulations benefits both licensees and consumers alike, aligning with our Bill of Rights, which emphasizes privacy protections for individuals.

NABIP does, however, offer one suggestion regarding the placement of the HIPAA/HITECH compliance exemption. Currently, the language is included in Article Seven, “Rules for Health Information,” since the original model (crafted before the finalization of the HIPAA privacy rules) only exempted those who were subject to and compliant with federal rules from the health information protections in what was then labeled Article Five. Given that the new language applies to the entire act, and not just one article, we suggest moving this section to Article Eight, “Additional Provisions,” for clarity.

While the vast majority of NABIP members will be exempt from the provisions of this model, as currently drafted, due to the HIPAA/HITECH privacy compliance exemption, some individuals and entities represented by our association may be subject to the provisions of Model #672 due to their business activities related to lines of insurance other than health. The current revisions to the model retain the definitions of health information and nonpublic personal health information that were included when it was originally drafted in 2001. At that time, the HIPAA privacy rules had not yet been finalized, and the HITECH data security rules were years away. Today, the definition of PHI, as established by HIPAA and HITECH, is well known to both consumers and industry professionals. For simplicity and clarity, we suggest that the Working Group replace the current health information definitions (and any other overlapping definitions) with those already established by HIPAA and HITECH privacy and data security rules.

Another recommendation NABIP offers, to make things easier for both state insurance department staff and those subject to the revised model, is to reinstate model notice language in the updated model. The original document included sample notice language for covered entities to use with consumers. This draft simply specifies that each state insurance commissioner will prepare a sample notice and post it online for licensees to use in notifying affected individuals. Including sample notice text in the model would allow for consistent notifications to be used nationwide and ensure the immediate availability of a compliant notice for licensees. This recommendation aligns with Article II of our Consumer Healthcare Bill of Rights, which stresses clear and consistent communication to consumers about their rights and protections.

Finally, regarding the entirely new Article Two, Section Five, “Third Party Contractual Obligations,” while we appreciate the notation that contract requirements be “consistent with the size and complexity of the third party,” this section goes on to specify many privacy protection elements that should be included in third-party contracts. Many contracts that licensees, particularly small business owners, are required to sign with third-party service providers are contracts of adhesion. Licensees, like the majority of insurance producers, often have little ability to modify these contractual arrangements. Rather than requiring licensees to ensure that service providers meet privacy standards by contract, NABIP believes it would be more appropriate for state regulators to address the activities of third-party service providers





directly, particularly when these providers accept sensitive information from insurance entities. This approach ensures fair treatment for smaller entities, as outlined in Article VI of our Consumer Healthcare Bill of Rights.

NABIP appreciates the NAIC's willingness to consider stakeholder comments in revising this critical model. If you have any questions or if NABIP can provide additional assistance as you continue developing this model, please do not hesitate to contact me.

Sincerely,

Jessica Brooks-Woods  
CEO, National Association of Benefits and Insurance Professionals (NABIP)

cc: Lois E. Alexander  
Jennifer Neuerburg

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

***Revisions to Model 672 - Chair's Working Discussion Draft (8/5/24 Version)  
Third-Party Service Provider Related Aspects (9/18/24 Deadline)***

***NAMIC Comments (9/18/24)***

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 exposure draft dated August 5, 2024 (draft). NAMIC members very much appreciate the efforts of the Privacy Protections (H) Working Group (PPWG or Working Group) and the ability to provide input.

Consistent with the direction of the Working Group, these comments focus on the aspects of the draft relating to third-party service providers. They are part of broader input, and we look forward to continuing to share members' concerns with other aspects of the draft as the process continues.

---

**THIRD PARTY CONTRACTUAL OBLIGATIONS  
Draft Article II: Section 5**

---

**ARTICLE & SECTION NAME**

As drafted, and as a technical matter, the focus of the draft's Article II and Section 5 do not seem to be limited to contractual provisions relating to third party service providers. If the scope is going to be broader, a more general title may aid reading and compliance.

---

<sup>1</sup> NAMIC Membership includes more than 1,450 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 \$391 billion in annual premiums. Our members account for about 68 percent of homeowners, 56 percent of automobile, and 31 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.



## CONTRACT REQUIREMENTS PROVISION-BY-PROVISION

### **Lead-in Language Sec. 5A**

The lead-in language in Section 5A would be improved by **more closely following the framing that is contained in Section 4A of Model #668**, which reads as follows:

Commensurate with the size and complexity of the Licensee, the nature and scope of the Licensee’s activities, including its use of Third-Party Service Providers, and the sensitivity of the Nonpublic Information used by the Licensee or in the Licensee’s possession, custody or control, each Licensee shall develop, implement, and maintain a comprehensive written Information Security Program based on the Licensee’s Risk Assessment and that contains administrative, technical, and physical safeguards for the protection of Nonpublic Information and the Licensee’s Information System.

**Scaling** requirements is appropriate because licensees, TPSPs, information, and activities may differ.

Also, more closely aligning the language of these models may **aid in implementation, compliance, and supervision**. For example, technically some may argue that “**commensurate with**” (from #668) and “consistent with” (from Chair’s draft) may be read to have different meanings. To avoid confusion and assessment under what some may consider possible divergent standards, it may be better to start with “commensurate with.” This is just one of several ways the wording could be modified for possible greater consistency.

*Revising and expanding lead-in wording in Sec. 5A :*

Commensurate ~~Consistent~~ with the size and complexity of the licensee and third-party service provider, the nature and scope of the activities of the licensee and the third party service provider, the type and sensitivity of the nonpublic personal information collected and processed by a third party service provider, and the third party service provider’s relationship with the licensee, a licensee that discloses a consumer’s nonpublic personal information to a third-party service provider shall enter into a contract with the third party service provider that:



### **Purpose Limitation Language in Sec. 5A(1)**

For consistency, consider using the full defined term, “third party service provider.”

*Making ministerial change in Sec. 5A(1) for internal consistency:*

Prohibits the third party [service provider](#) from processing the nonpublic information for any purpose other than those related to providing the services specified in the contract with the licensee, unless retention is necessary to comply with the law or valid and binding order ~~of~~ a governmental body;

As a ministerial item, it appears that “a governmental body” should be preceded by “of” rather than “or.”

There was some member input received that this provision includes multiple concepts – (1) purpose limitation; and (2) expectations around retention – and there may be benefits to separating them into separate provisions.

Also, as the drafting process continues, we may have additional suggestions relating to additional exception wording to follow “unless.” For example, there may be additional thoughts around record retention and/or fraud prevention. We appreciate any flexibility to offer additional input on these and other items as the PPWG’s drafting process moves forward.

### **Deletion/Return Language in Sec. 5A(2)**

A number of questions arose as members reviewed wording relating to the contractual provision which would **always mandate deletion and return of nonpublic personal information**. There may be a need to allow for some flexibility to handle those situations in which, as a practical matter, this may not be able to happen. For example, consider when removal from archives may require additional operational processes to first restore an entire system since it may not be feasible in some instances to delete selectively. These concerns must be addressed, and existing legal and regulatory approaches may offer some useful direction.

To illustrate, **New York** Department of Financial Services provides an example of such wording through Section 500.13 which refers to “where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.” The idea of “compensating controls” is also included in portions of Regulation 500 and may be worthwhile to consider in this context as well. And, though somewhat different, **California** also provides for some level of flexibility in Sec. 1798.105(c)(3) as it contains exception wording that references deletion “unless this proves impossible or involves disproportionate effort.” Further, **other laws** relating to document disposal/destruction may also be instructive.



Rather than addressing all these concepts in Section 5A(2) itself, which may needlessly complicate the wording around contractual requirements, please consider adding a **new definition of “delete”** to Section 4, which we believe will benefit the draft overall. The following aims to share a language that may address situations described above and incorporate the ideas set forth in the highlighted state law/regulation examples:

*Adding definition of “delete” to Section 4 to aid practical compliance with Sec. 5A(2):*

- (1) “Delete” means secure disposal of nonpublic personal information by taking measures reasonably expected to protect against unauthorized access to or use of the information in connection with its disposal.
- (2) Examples of measures reasonably expected to protect against unauthorized access to or use of nonpublic personal information in connection with disposal include but are not limited to:
  - (i) Rendering the nonpublic personal information unreadable or indecipherable, such as through destroying, shredding, burning, pulverizing, erasing, or otherwise modifying so that the information cannot practically be read or reconstructed.
  - (ii) Implementing appropriate compensating controls, either when targeted disposal is not reasonably feasible due to the way the information is maintained or when deletion proves impossible or involves disproportionate effort.

Returning to the wording in Section 5A(2) – and assuming the substantive concerns are addressed through a new definition – the TPSP also likely has its own **record retention** policies. Also, as a technical matter, it may enhance readability to break this provision into component parts, such as:

*Expanding Sec. 5A(2) to allow for practical items:*

Obligates the third-party service provider, at the licensee’s direction, to delete or return all nonpublic personal information to the licensee:

- (a) When requested; or ~~to delete information~~
- (b) After it is no longer necessary either to fulfill a legal requirement or to meet their record retention requirements.

Similar to above, it may be that additional consideration should be given to certain situations relating to fraud prevention/monitoring. We appreciate the ability to continue to provide feedback on this and other items as the PPWG drafting process continues.



### **Noncompliance and Termination in Sec. 5A(3)**

Different perspectives inform our suggestion provided in response to Section 5A(3). Consider:

- Potential for changing negotiation dynamics during a **contractual re-write** process that may prompt possible push back and may invite demands – as once the door is open to renegotiate the contract wording, TPSPs may seek to modify other wording unrelated to privacy (and to the relative detriment of the licensee).
- Existing contractual noncompliance wording (that may be broader than privacy-related aspects of a licensee’s contract with a TPSP) should not be disrupted by requiring certain **placement of provisions** or wording to be bundled together with privacy-related provisions.

Given these concerns, we ask the PPWG to please consider the following alternative:

*Revising Sec. 5A(3) to avoid disruption and adding an example:*

Obligates the third-party [service provider](#) to notify the licensee if it can no longer comply with its [contractual obligations regarding privacy as well as handling and safeguarding nonpublic personal information under this agreement](#) and provides the licensee with a right to terminate the agreement in such case;

[\(#\) Example of contracts satisfying the requirement to include a provision relating to a licensee no longer complying with obligations. Nothing in this subsection shall be construed as requiring a privacy-specific provision, as long as the contract obligates a third party service provider to notify the licensee of a failure to comply and allows the licensee the option to terminate the agreement.](#)

The suggested wording above aims to offer clarity and flexibility to address these concerns.



### **Subcontractors & Copies of ALL Subcontractor Agreements in Sec. 5A(4)**

The requirement for every third party service provider to provide all its subcontractor agreements to every licensee with whom it does business would be incredibly **inefficient** for all parties involved.

It further **assumes that TPSPs would agree – or even be able to agree** – to provide copies of such agreements. As a practical matter, they may refuse (especially large important providers) because of factors such as their own contractual obligations to retain them as confidential and/or to protect trade secrets. For example, they may be unwilling to disclose factors such as pricing and service levels that may be embedded in such contracts.

Further, as we understand it, as a matter of **precedent**, this kind of requirement is not contained even within HIPAA and CCPA (both of which also include the concept of requiring data processors to have contracts in place with subcontractors).

Of course, as an administrative matter throughout, where applicable the **defined term** “nonpublic personal information” should be used consistently rather than simply “personal information” in some places (which may introduce possible confusion). (And as indicated below, it is important that the revisions to the “nonpublic personal information” definition be reviewed in the context of contracts with TPSPs and other aspects of the draft.)

Because of these reasons, the end of this provision should be removed and we ask that other ministerial edits be made.

*Removing last portion of Sec. 5A(4) to avoid disruption and inefficiencies:*

Obligates the third party to enter into written agreements with subcontractors that include provisions requiring them to meet the privacy obligations of the third-party service provider with respect to nonpublic personal information ~~and provide copies of those contracts to the licensee;~~

While one member suggested a possible alternative of inserting “upon the licensee’s request” before “and provide copies of those contracts to the licensee,” may address the inefficiencies, it still would be expected to be met with strong opposition on the other grounds outlined above. Again, please remove the requirement for TPSPs to provide the licensee with copies of subcontractor contracts.



Members indicated that there should be some flexibility in the way in which their contracts may be worded. Specifically, some concern was expressed about potential ambiguity and resistance to the wording “requiring them to meet the obligations of the third-party service provider with respect to personal information.” While members will continue to think about alternatives, kindly consider this as an area where **examples** of what could constitute compliance could be helpful. Possible additional wording for consideration follows:

*Adding Example to Sec. 5A(4) to avoid disruption and inefficiency:*

[\(#\) Example of contracts satisfying the requirement to include a provision relating to a licensee requiring subcontractors to meet obligations relating to nonpublic personal information. An obligation for the third party to enter into written agreements with subcontractors that contains provisions no less protective of the nonpublic personal information than those contained in the third-party service provider’s agreement with the licensee shall satisfy this requirement.](#)

Such wording may also **align** with the confidentiality provisions in contracts. Consider that HIPAA requires business associates’ contracts with their subcontractors to include the same restrictions and conditions applicable to the business associate.

### **Assisting with Consumer Requests in Sec. 5A(5)**

On its face, this provision seems relatively reasonable, it may be that there should be consideration of where the TPSP has its own **independent business relationship** with a consumer that may warrant some level of exception to both the Section 6 relating to consumer requests and to this provision. Making this allowance explicitly – perhaps via an example - may acknowledge some of the complexity and nature of these situations.

### **Safeguards & Breach in Sec. 5A(6)**

This provision tries to address different issues – safeguards and breach – and if moving forward with both, they should be addressed separately in separate provisions. (Although as indicated below, there are substantive concerns with the inclusion of each.)





### Security Safeguards

Overall, including this provision in this model **risks conflating privacy with security**. Section 5A(6) deals with data security and “administrative, technical, and physical safeguards” wording stems from the security related wording from Gramm-Leach Bliley and it has been carried through and expanded upon in the NAIC’s Model #668, the Insurance Data Security Model Law, including with respect to TPSPs.

Indeed, today **Model 668 already addresses requiring TPSPs to have these security measures**. Section 4F(2) of that model reads as follows:

A Licensee shall require a Third-Party Service Provider to implement appropriate administrative, technical, and physical measures to protect and secure the Information Systems and Nonpublic Information that are accessible to, or held by, the Third-Party Service Provider.

Because this is security related and there is a provision in #668, we encourage the PPWG to remove this provision in its entirety.

*Removing Beginning of Sec. 5(A)(6) [to cut security aspects from privacy model]:*

~~Obligates the third-party to implement and maintain reasonable administrative, technical, and physical data security practices to protect the personal data from unauthorized access, destruction, use, modification, or disclosure, ...~~

If the PPWG wishes to retain the provision, we strongly urge for the same wording to appear in both models. Not only might this aid in interpretation (for implementation and market conduct), but these aspects of contracts should not need to be rewritten. As it stands, for the first portion of the new provision, the wording differs -- #668 says “implement appropriate” and this draft says “implement and maintain reasonable.” In no case should the provisions differ; and ideally there would not be security provisions in the privacy model. The PPWG should avoid confusion:

*Revising Beginning of Sec. 5A(6) [alternative and consistent with Model #668]:*

Obligates the third-party service provider to implement appropriate and maintain reasonable administrative, technical, and physical data security practices to protect the nonpublic personal information data from unauthorized access, destruction, use, modification, or disclosure, ...



## **Breach**

The draft also **references “breach”** along with a time period. This has sparked significant speculation and questions, including:

- Isn't this really **duplicative** with the **noncompliance provision in draft Section 5A(3)**? Please see above and consider whether this topic is adequately addressed such that this provision can be removed.
- **What does “breach” mean in this context?** In terms of scope, is the intent to address breach of contract or breach of security? On its face, it would appear to relate to breach of contract. Regardless, again, it appears that draft Section 5A(3) would address this concern.
- **Does this conflate security and privacy and isn't the former already the subject of Model 668?** If not necessary, consider removing it here as it adds unnecessary confusion and complexity.
- To the extent that this relates to a **notification of a cybersecurity event type breach** relating to nonpublic personal information (which does not appear to be what the draft actually refers to), in addition to the concerns above, consider the following:
  - There are several concerns such as **defining specific thresholds/standards for triggering** the obligations (and aiding understanding of the commitments, such as when the clock begins to run, etc., and whether it relates to things like unauthorized acquisition of and access to nonpublic personal information). There are no such definitions included in this model.
  - There are also concerns with the **time periods**. This should be an area that allows licensees to have some flexibility to engage their TPSPs when it comes to contractual wording. A 48 hour mandate may be met by substantial TPSP resistance (and it does not appear to account for non-business days). As a practical matter, consider all of the work that is prompted by an incident and the likelihood that some TPSPs may insist on first confirming a security breach (and this for some licensees, this may be a step backwards with respect to their TPSP agreements).

Importantly, also consider that the 48 hours may differ from the timeframe under general laws. The Securities and Exchange Commission also considered a 48 hour timeframe and conclude that it was inconsistent with other regulations. (Compare the final and proposed rules.)

Further, in New York, the Department of Financial Services has imposed an already ambitious 72 hour period. See Reg. Sec. 500.17(a)(1).



If the PPWG finds that it must go forward with this provision, we understand that HIPAA requires notice “promptly and without unreasonable delay” following a “discovery” (a defined term) of a security incident. See 45 CFR Sec. 164.410.

Based on all of these concerns, we strongly urge removing the second portion of this provision in its entirety.

*Removing End of Sec. 5A(6) [to resolve challenges/redundancy/confusion]:*

~~... and require notification to the licensee of a breach of this term within 48 hours.~~

If the PPWG feels that such a requirement must be maintained, while we continue to talk with members about this approach, the following wording may incorporate an approach similar to HIPAA and may be less problematic (though still concerning):

*Revising End of Sec. 5A(6) [concerning alternative]:*

... and require notification to the licensee of a breach promptly, and without unreasonable delay from [trigger] of this term within 48 hours.

Or, as a less preferred alternative, if the PPWG feels it must include a timeframe, this may blend some of the HIPAA and New York approaches using 72 hours:

*Revising End of 5A(6) [more problematic alternative]:*

... and require notification to the licensee of a breach promptly, and in no event longer than 72 hours following [trigger] of this term within 48 hours.

Again though, before looking to amend Section 5A(6) wording, we respectfully ask the Working Group to consider both whether: (1) it is necessary to include security-related provisions in privacy-related contractual provisions (where this is already contemplated in Model #668); and (2) the other noncompliance provision in this draft – specifically in Section 5A(3) – already addresses these concerns adequately. To avoid the many questions and concerns, we strongly urge the Working Group to please remove all of Section 5A(6).



## ADMINISTRATION & HANDLING PROVISION

The portion of Section 5 that deals with third party service provider arrangements other than the contract requirements in (A) is causing confusion and angst. In looking at **Section 5B**, consider a few examples.

- The “**solely**” wording is raising concerns of possible interpretations **limiting the ability to hold a TPSP liable to a licensee** (or restricting TPSPs indemnifying a licensee), whether contractually or through litigation. This interpretation and possible outcome would be negative and highly problematic.
- The **meaning of “administration of its data integrity”** is unknown and is raising questions. This ambiguity and confusion should be avoided.

To avoid confusion, we suggest removing this section:

*Removing 5B:*

~~The licensee is solely responsible for the administration of its data integrity and compliance with this Act and the handling of nonpublic personal information.~~

We are continuing to consider what would be an appropriate alternative suggestion, if the PPWG feels it needs to move forward with another provision in Section 5. One possibility may be as follows:

*Addition to 5B (if unwilling to remove altogether):*

Due Diligence. A licensee shall exercise reasonable risk-based due diligence in selecting its third party service providers.

This would align with NAIC Model #668, the Insurance Data Security Model Law, Section 4(F)(1) which requires a licensee to exercise due diligence in selecting its third party service provider.

## CHALLENGES WITH PRESCRIBING CONTRACTUAL PROVISIONS & POSSIBLE ALTERNATIVE

While recognizing that contract-related wording was contained the proof of concept 672-Plus version, there are general concerns that members feel must be conveyed to the Working Group. In general, when laws become more prescriptive, such that licensees would need to amend contracts - which likely are already contain adequate privacy-related provisions - for the sake of technical compliance with very specific items, it introduces a risk of the service providers seizing the opportunity to insist on modifying other protections a licensee has in its contracts unrelated to protection of data (possibly increasing financial risk). Questions were raised about the rationale for (and what problems prompt) regulating third party service provider agreements, especially with this level of detail.

The Working Group can take **several steps to mitigate this risk**:

- (1) Keeping the provisions in Section 5A fairly **high-level** (and removing/modifying wording such as encouraged above);
- (2) Implementing only on a **go-forward basis for new contracts** and being clear about delays with a separate Section 5 related effective date provision (such as sketched below); and
- (3) Developing an **optional template or sample provisions** – even if after the Model is finalized – and building-in a possible safe harbor (or compliance deemer) for use of that template or those provisions if ever developed.

With respect to this last point, from an operational uniformity perspective, such optional wording could offer significant efficiencies.

- As a future step, consider the possible value of an NAIC crafted **optional safe harbor template data processing agreement (DPA)**. Such wording may be helpful in situations in which some service providers may be pushing back or refusing new contractual assurances, as we understand may have been a dynamic in response to CCPA and other U.S. privacy laws.
- **Sample wording** is pointed to as one of the things that aided in the success of rolling out all the notices when Model #672 was first adopted. The sample wording did not vary from state-to-state – operational uniformity is crucial, especially where the contracts with TPSPs may not relate to services relating to a single state. (At the appropriate time, NAMIC expects to provide input on retaining this idea with respect to notice, etc.) While we recognize that the Working Group may be concerned with finalizing the draft itself and not want to get into the work of developing templates and/or sample clauses, perhaps it can build-in springing wording to hold this option for a future Working Group change.



While we are continuing to think about the possible ways to structure this concept, one idea presently under consideration would be adding examples to apply to Section 5A overall and might look something like the following:

*Adding Examples and Optional Compliance Deemer Possibility for Section 5A:*

Examples of contacts and provisions that comply with Section 5A. To the extent applicable, use of any of the following, if adopted by the National Association of Insurance Commissioners is incorporated by reference, shall constitute compliance with the third party service contractor agreement requirements of this Act:

- (#) A template or model agreement;
- (#) A sample contractual provision; or
- (#) An example.

Use of these National Association of Insurance Commissioner materials is not required. Licensees may use other agreements and other provisions, provided that they meet the requirements of Section 5A.

Given the “if adopted” wording, the idea is to allow for the possibility that the PPWG could work on such wording in the future (and with enough time to allow for contract negotiation before the Section 5 effective date).



## TERMINOLOGY

While the defined term in the draft's Section 4CC is "third party service provider," that **term is not used consistently** in Section 5. To aid consistent interpretation, please replace "third-party" with third party service provider throughout Section 5. There is concern that using different wording may mean that some interpret the phrase to mean something different and that the scope could somehow be seen as broader (such as including affiliates, for example).

While members are still considering it, perhaps in the alternative it could be effective to refer to the full "third party service provider" wording in targeted places for the same meaning:

### *Adding Wording to Clarify TPSP Scope/Consistency in Sec. 5:*

- Title for Article II: Third Party [Service Provider](#) Contractual Obligations
- Heading for Section 5: Third Party [Service Provider](#) Arrangements
- Lead in Language in A: Contract Requirements. Consistent with ... of the third party [service provider](#), a licensee... to [a such](#) third party service provider shall enter into a contract with the third party [service provider](#) that:

This up-front wording may aid all stakeholders in interpreting the requirements that follow to relate only to defined third party service providers. We are continuing to review this approach but offer it here in case the PPWG has resistance to changing the wording throughout Section 5.



---

**“THIRD PARTY SERVICE PROVIDER” DEFINITION**  
**Draft Section 4CC**

---

While considering the substantive provisions (in new Article II (Section 5) relating to third party contracts or arrangements), it seems timely to consider the corresponding definition for “third party service provider.” Largely, the definition accounts for what should and should not be included as a TPSP. However, there is one entity missing that is essential to account for within the definition. Specifically, **government entities** should be excluded because of a number of reasons.

- When a licensee must provide information to a governmental entity, there may be times where there may be barriers to obtaining a contract, especially one containing all the substantive provisions that would be required under the draft’s Section 5A. It may put the licensee in a difficult negotiating position as it may mean that they may be put between different potential non-compliance pressures (for whatever request and for the contract under the model), especially if deadlines are short.
- Whether information is compelled in response to a breach or in connection with some other examination, compliance, or other legally authorized activity, the model should account for those situations.
- Under Sections 21-22 (previous Sections 17-18) which outlines certain exceptions for disclosure of nonpublic personal information, responding to government requests is listed.

The PPWG could address these concerns by **expanding the “third party service provider” definition** by adding wording along the lines of adding the following:

*Adding Language to TPSP Definition to Clarify Scope:*

Entities not included. Third party service provider does not include a government entity

*or*

(1) Is not a government entity.

Incorporating such an approach may enhance the future workability for regulators and licensees alike.



---

### THIRD PARTY CONTRACTS & EXCEPTIONS

#### Draft Section 19A (current Model 672 Sec. 15A)

---

The existing model contemplates contracts with third parties within the opt out exception found in Sec. 15A(1)(b) and this concept is rightly retained in Section 19A(1)(b) of the draft. However, it given the draft's new addition of a subsection to provide for greater details relating to TPSP contracts, the exception language can now be **streamlined** to simply reference that subsection (Section 5A).

To account for moving (and expanding) the wording, consider modifying draft Section 19A along the lines of the following:

*Revising Sec. 19A [to account for new Sec. 5A and its contract-related requirements]:*

Section 19(A)(1)...

(b) Enters into a contractual agreement with the third party [consistent with Section 5A](#) ~~that prohibits the third party from disclosing or using the information other than to carry out the purposes for which the licensee disclosed the information~~, including use under an exception in Sections 20 [previously 16] or 21 [previously 17] in the ordinary course of business to carry out those purposes.

The new draft incorporates a purpose-related TPSP limitation in Sec. 5A(1) and then the draft expands the contractual requirements that would be required under an updated model. Therefore, the longer wording is not needed here, and it seems this provision can simply refer back to the corresponding new provision in Section 5.



---

**THIRD PARTY SERVICE PROVIDER AGREEMENTS & EFFECTIVE DATE**  
**Draft Section 32 (current Model 672 Sec. 27)**

---

When considering substantive licensee requirements relating to TPSPs, please appreciate realities:

- The **magnitude of the effort and time** required to manage the significant task of modifying contracts to bring them into compliance with newly articulated requirements.
- The real challenges associated with **renegotiating with TPSPs** to modify existing and validly executed agreements with previously agreed upon wording.

To reduce some of the implementation burden associated with the TPSP requirements in Section 5, we ask that the PPWG’s model:

- Set a **delayed** effective date, consistent with when GLBA and Model 672 was first implemented. See draft Section 32 (though some hear that “grandfathering” wording could be modernized). Two years seems reasonable based on historical approaches as well as the size of the project. That said, if the NAIC is thinking of crafting optional template agreements/provisions that timeline may be relevant to consider as well.
- New requirements should **apply only to go-forward agreements**. This is reasonable because, unlike when #672 was first passed, there have now been long-standing legislative/regulatory requirements around purpose and confidentiality provisions in contracts with TPSPs.

Specifically, possible wording with respect to the TPSP contract effective date follows:

*Revising Sec. 32 [to account for TPSP contract processes]:*

C. [Third-party service provider agreements.](#)

(1) [A new contractual agreement with a third party service provider:](#)

(a) [If entered into after two years from the general effective date in Subsection A of this Section, such agreement must meet all the requirements of Section 5.](#)

(b) [If entered into after the general effective date in Subsection A of this Section, but before two years from that general effective date, such agreement must at least meet the requirements of Section 5A\(1\) and shall be deemed to satisfy the remaining requirements of Section 5, even if the contract does not include provisions that meet all the requirements of that Section.](#)

(2) [A pre-existing contractual agreement entered into on or before the general effective date of Subsection A of this Section shall be deemed to comply with the requirements of Section 5, even if the contract does not meet all the requirements of that section.](#)

Two-year grandfathering of service agreements. Until [\[Insert Date\]](#) July 1, 2002, a contract that a licensee has entered into with a nonaffiliated third party to perform services for the licensee or functions on the licensee’s behalf satisfies the provisions of Section 195A(1)(b) of this Act regulation, even if the contract does not include a requirement that the third party maintain the confidentiality of nonpublic personal information, as long as the licensee entered into the agreement on or before [\[Insert Date\]](#) July 1, 2000.

This language aims to minimize disruption while also moving forward with new agreements.



---

## LIMITED EXEMPTION Draft Section Missing

---

As the PPWG considers adding new provisions to expand licensee requirements beyond those required under Gramm Leach Bliley Act, as implemented by insurance regulators under Model #672, please consider the impact on smaller licensees. Specifically, new requirements relating to contracts with third party service providers may be among those areas where a limited exemption should apply. Indeed, as the comprehensive privacy laws have been passing in the states, smaller entities have been exempted. Consider a size based exemption – such as one that includes “[a licensee that processes the nonpublic information of less than thirty-five thousand resident consumers during a calendar year](#)” – as a way to recognize the impact on smaller licensees. Such limited exemption would not apply cross-the-board, but to listed additional new requirements.

---

## CONSUMER REQUESTS FOR ACCESS, CORRECTION, AND DELETION OF NPPI Draft New Section 6

---

While considering the substantive provisions (in new Article II (Section 5) relating to third party contracts or arrangements), perhaps it is timely to reference a concern with a provision referencing third party service providers in Section 6(A)(1)(a)(i) which would require insurers to provide “a list of all third-party service providers ...” Rather than such a list, please consider referencing “categories” because of several practical reasons.

- First, such lists may have the potential to have negative impacts such as by outlining information that could introduce **security threats** and/or may **hinder competition**.
- Second, categories would be less **overwhelming**, and the content would be more **evergreen**.

For these reasons, please consider this change:

*Revising Sec.6A(1) [on TPSP related information provided upon request]:*

Must include [the categories](#) ~~a list~~ of all third-party service providers to ~~in~~ which the licensee disclosed the consumer’s nonpublic personal information; and

An approach requiring a list of categories of third parties is **more consistent with the general approach that is more prevalent in state privacy laws**. For example, consider the Delaware Personal Data Privacy Act along with California (CCPA) (and others with comprehensive laws that require controllers to list the categories of third parties to which they disclose personal information generally).



---

**OTHER DEFINITIONS**  
**Section 4**

---

As the PPWG drafting process continues, it may be that the substantive requirements in Section 5 relating to TPSPs are impacted by the definitions and/or have implications for other sections.

For example, consider the change to the definition of “**nonpublic personal information**” (NPPI) (numbered as V in the discussion draft). Given how the definition now reads and the reference to (or intended reference to) NPPI within the TPSP section, the contractual provisions might technically be read to sweep in publicly available information. The reasonable wording pointing to “**publicly available**” is within the definition of “nonpublic personal financial information” of the existing Model #672 and which is not imbedded in the NPPI definition in this draft. It is essential that “nonpublic personal information” not encompass publicly available information. These kinds of practical technical issues are extremely important to consider.

NAMIC respectfully asks for the opportunity to continue to offer feedback on definitions and other matters as the process continues to move forward.

\* \* \* \* \*

In conclusion, the draft offers a strong starting point for the TPSP topic and NAMIC asks that the practical issues raised in these comments be considered because they are reasonable ways to enhance compliance with the draft while protecting consumer privacy. As the language in the draft, and member understanding of it, continues to evolve, NAMIC may have additional input on aspects relating to TPSPs.

The current direction to stakeholders was to focus initial comments on this particular topic, which NAMIC has done here. As the PPWG welcomes feedback on other portions of the model, NAMIC is eager to engage on those as well. Finally, please understand that the input shared here is based on current input and that review and thought on these matters will continue and therefore feedback may evolve over time. On behalf of members, thank you for this opportunity.

**From:** [Alexander, Lois](#)  
**To:** [Christian Grofcsik](#)  
**Subject:** RE: DRAFTING GROUP VOLUNTEER - Privacy Protections Working Group  
**Date:** Friday, August 23, 2024 9:15:00 PM  
**Attachments:** [image001.png](#)

---

Hi Christian,

Thank you for volunteering. I will add your name to the list for consideration by the chairs. I will also send your comment to them for use with the drafting group. Comments will be posted after the deadline.

Best,  
Lois

**Lois Alexander**  
Manager II – Market Regulation  
Regulatory Services

**O:** 816-783-8517  
**M:** 913-244-9484  
**W:** [www.naic.org](http://www.naic.org)

---

**From:** Christian Grofcsik <[christian.g@nextinsurance.com](mailto:christian.g@nextinsurance.com)>  
**Sent:** Thursday, August 22, 2024 6:04 PM  
**To:** Alexander, Lois <[LAlexander@naic.org](mailto:LAlexander@naic.org)>  
**Subject:** DRAFTING GROUP VOLUNTEER - Privacy Protections Working Group

**CAUTION:** This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hi Lois Alexander,

I would like to volunteer to the Privacy Protections Working Group.

My information:

Christian Grofcsik  
Associate General Counsel  
Next Insurance  
[christian.g@nextinsurance.com](mailto:christian.g@nextinsurance.com)  
561-715-4562

I also had a comment on the Section being reviewed. I hope this isn't an inappropriate method to bring this up, but the email forwarded to me did not describe how to provide comments.

II.5. Third Party Arrangements

Comment:

The notice of non-compliance of A(3) and A(6) could be combined in A(3) and I

suggest that A(6) require notice in the event of such an unauthorized disclosure, which wasn't addressed in this section but would be a critical obligation of a third party to ensure prompt response to any unauthorized disclosure.

Suggestion:

...

(3) Obligates the third-party to notify the licensee within 48 hours **if it breaches or** if it can no longer comply with **its-any obligations** under this agreement and provides the licensee with a right to terminate the agreement in such case;

...

(6) Obligates the third-party to implement and maintain reasonable administrative, technical, and physical data security practices to protect the personal data from unauthorized access, destruction, use, modification, or disclosure, **and require notification to the licensee of a breach of this term within 48 hours** and requires **notification of any unauthorized access, destruction, use, modification, or disclosure of personal data within 48 hours.**

My best regards,

**Section 5. Third Party Arrangements**

A. Contract Requirements. Consistent with the size and complexity of the third-party, a licensee that discloses a consumer's nonpublic personal information to a third-party service provider shall enter into a contract with the third-party that:

(1) Prohibits the third-party from processing the nonpublic personal information for any purpose other than those related to providing the services specified in the contract with the licensee, unless retention is necessary to comply with the law or valid and binding order or a governmental body;

(2) Obligates the third-party at the licensee's direction, to delete or return all nonpublic personal information to the licensee when requested; or to delete personal information after it is no longer necessary to fulfill a legal requirement;

(3) Obligates the third-party to notify the licensee if it can no longer comply with its obligations under this agreement and provides the licensee with a right to terminate the agreement in such case;

(4) Obligates the third-party to enter into written agreements with subcontractors that include provisions requiring them to meet the obligations of the third-party service provider with respect to personal information and provide copies of those contracts to the licensee;

(5) Obligates the third-party to provide reasonable assistance to the licensee in fulfilling obligations to respond to consumer requests under Article III of this Act.

(6) Obligates the third-party to implement and maintain reasonable administrative, technical, and physical data security practices to protect the personal data from unauthorized access, destruction, use, modification, or disclosure, and require notification to the licensee of a breach of this term within 48 hours.

B. The licensee is solely responsible for the administration of its data integrity and compliance with this Act and the handling of nonpublic personal information.

**SUGGESTED REVISED LANGUAGE:**

**Section 5. Third Party Service Provider Arrangements**

A. Contract Requirements. Any contract between a licensee and a third-party service provider that involves the disclosure of a consumer's nonpublic personal information shall:

(1) Prohibit the third-party service provider from using or disclosing the nonpublic personal information for any purpose other than related to providing the services specified in the contract with the licensee unless retention is necessary to comply with the law or valid and binding order of a governmental body.

(2) Require the third-party service provider, at the licensee's direction, to delete or return all nonpublic personal information to the licensee when requested by the licensee unless retention is necessary to fulfill a legal or contractual requirement.

**Commented [FJ1]:** The terminology changed from "third party service provider" which is a defined term to "third party." Assuming these are not meant to be different, suggest either changing the terminology in the section or the definition so they are consistent.

**Commented [FJ2]:** The effective date of this section is unclear, but this does not appear to fall within the effective date requirements of section 32, which apply only to section 19 In PA, for example, applying requirements retroactively to contracts raises constitutionality concerns.

Suggest making a note to address contracts in the effective date provisions when those are finalized, adding language such as "For contracts entered into, amended, or renewed on or after the effective date of this act..."

**Commented [FJ3]:** It seems as if not all these requirements should be dependent on the size and complexity of the third party. Suggest that 6 would be?

**Commented [FJ4]:** The language "shall enter into a contract with the third party that" suggests that the parties must enter into an additional contract containing the required terms, instead of those terms being added to the main contract. Was this the intent? It seems cleaner to require the provisions in one contract, or at least leave the option open to the parties.

**Commented [FJ5]:** Should this say "binding order OF a government body"?

**Commented [FJ6]:** Was the intent of this provision to require deletion UNLESS it is necessary to fulfill a legal requirement? This needs to be reworded or this provision would require automatic deletion.

**Commented [FJ7]:** The term "reasonable" would raise vagueness concerns in PA.

**Commented [FJ8]:** The term "reasonable" would raise vagueness concerns in PA.

**Commented [FJ9]:** Suggest that breach notification should be broken out in its own paragraph since it is a separate requirement.

**Commented [FJ10]:** Is the intent of this paragraph to provide that even if the licensee contracts with a third party for a service it may not delegate its statutory obligations under the Model Law with regard to the data? Or is the intent to hold the licensee responsible for the subcontractor's misuse of the data? Or both?

(3) Contain a provision requiring the third-party service provider to honor a consumer's directive to opt in or opt out of the provisions under this act.

(3) If the third party is no longer able to comply with its obligations under the contract:

- (i) Require the third-party to notify the licensee; and
- (ii) Provide the licensee with a right to terminate the contract.

(4) Require that any contract between a third-party service provider and a subcontractor of the third-party service provider with access to a consumer's nonpublic personal information meet the following criteria:

- (i) Be in writing;
- (ii) Contain a provision requiring the subcontract to meet the requirements for treatment of nonpublic personal information under this act; and
- (iii) Be forwarded to the licensee within X days of the effective date of the subcontract.

(5) Require the third-party service provider to assist the licensee in fulfilling obligations to respond to consumer requests under Article III of this Act.

(6) Obligate the third-party service provider to implement and maintain administrative, technical, and physical data security practices commensurate with the size and complexity of the third-party service provider to protect the personal data from unauthorized access, destruction, use, modification, or disclosure.

(7) Require the third-party service provider to provide notification to the licensee of a breach involving nonpublic personal information of the licensee's consumers within 48 hours.

B. A licensee may not delegate responsibility for the administration of its data integrity and compliance with this Act to a third-party service provider and shall be responsible for a third-party service provider's use of consumer data that does not comply with the requirements of this act.



September 17, 2024

Amy Beard, 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 on the Chair Draft Amendments Section 5 – Third-Party Arrangements

Dear Commissioner Beard,

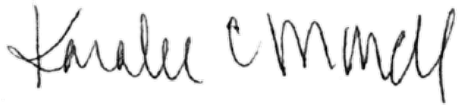
The Reinsurance Association of America (RAA) appreciates the opportunity to submit comments to the Privacy Protections (H) Working Group on Section 5 – Third-Party Arrangements of the recently exposed Chair Draft amendments to the NAIC Insurance Information and Privacy Protection Model Act (#670). The Reinsurance Association of America (RAA), headquartered in Washington, D.C., is the leading 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 thanks the Working Group for its continued thoughtful engagement in updating the model act. As indicated in our previous letters to the Working Group (dated August 7, 2023, July 27, 2023, and April 3, 2023), the RAA previously had a number of concerns with the various drafts of the Working Group's then proposed new model law. After the last exposure draft of the then proposed new model, the RAA had one remaining significant reinsurance-related concern, the extent to which reinsurers would fall within the definition of third-party service provider. The RAA is pleased that this concern has been rectified in the new Chair Draft and supports that in the Chair Draft reinsurers are not considered third parties. This is a welcome change from the previous attempt to draft a new model law and the RAA applauds the Working Group's ongoing attempts to listen and engage with stakeholders in this complicated and valuable process.

The RAA looks forward to continuing to work with you on this important project and fully supports the decision to not consider reinsurers third parties under the Chair Draft. 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.

Should you have questions, please contact Karalee Morell ([morell@reinsurance.org](mailto:morell@reinsurance.org) or 202-783-8380).

Sincerely,



Karalee C. Morell  
SVP and General Counsel  
Reinsurance Association of America

**From:** Alexander, Lois  
**Sent:** Wednesday, September 18, 2024 11:26 AM  
**To:** Marnell, Frank <Frank.Marnell@state.sd.us>  
**Cc:** Neuerburg, Jennifer <JNeuerburg@naic.org>; Weatherford, Holly <hweatherford@naic.org>; Privacy Protections Working Group <privacywg@naic.org>  
**Subject:** RE: Privacy Protections (H) Working Group - Notice of Public Exposure of Chair Draft Accompanied by Drafting Group Guidelines

Good morning, Frank.

Thank you for submitting South Dakota's comments to Section 5 Third Party Arrangements within this email and for volunteering for the drafting group.

We look forward to productive meetings.

Sincerely,

**Lois Alexander**  
Manager II – Market Regulation  
Regulatory Services

**O:** 816-783-8517  
**M:** 913-244-9484  
**W:** [www.naic.org](http://www.naic.org)

**From:** Marnell, Frank <Frank.Marnell@state.sd.us>  
**Sent:** Tuesday, September 17, 2024 4:22 PM  
**To:** Alexander, Lois <LAlexander@naic.org>  
**Subject:** RE: Privacy Protections (H) Working Group - Notice of Public Exposure of Chair Draft Accompanied by Drafting Group Guidelines

**CAUTION:** This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Lois,

The South Dakota Division of Insurance is encouraged by the Chair Draft Amendments to #672 as an important starting point for revisions in general. Specifically, the Division supports the limited framework presented in Section 5 as a step towards a sensible, minimum, uniform model for third-party accountability.

- Subsection A: Licensees across the regulatory landscape conduct business with varying complexity in diverse markets, making flexible language necessary in Subsection A. Regulating the conduct of non-licensees through regulations about licensee contracts is not a new concept, but regulations like this should not be blanketly indiscriminately across the industry. Without detailed evidence of actual privacy abuses by industry to perform a fair analysis, it is difficult to establish the appropriate thresholds to mandate new regulations above or below an arbitrary point. A case-by-case analysis is therefore advisable at this time, as encouraged by this language. If real abuses are seen after NAIC passage and broad state enactment, this model can

be reopened to add definitive thresholds for mandating licensee contracting behavior in Subsection A. The group should consider additional third-party contract protections suggested in other comments to be added in the numbered paragraphs under Subsection A if the group agrees.

- **Subsection B:** The South Dakota Division of Insurance is in strong support of the new language in Subsection B concerning licensee responsibility for the administration of data integrity and compliance with the Act. This is similar to existing language in the NAIC model regarding licensee oversight of third-party administrators, which is already in practice. The language would hold licensees generally accountable to regulators for third-parties who handle sensitive consumer information. The language also reduces the need to draft extensive regulatory schemes to cover all third-party concerns at this time. Responsibility for a privacy protection failure by a third-party under more specific requirements elsewhere in the draft would be answered by the applicable licensee(s). A privacy complaint would trigger the regulator to use new Subsection B to initiate an investigation or examination directed at its answerable licensee rather than some nebulous third-party. The regulator would identify any regulatory violations that occurred under the more specific requirements of the Act using the Department's existing authority, then use the data to assist consumers and protect the public through action. That state data, developed over time, will inform regulators as to revisions to subsection A of Section 5 based on real cases. This is a reasonable approach to evolving regulations in an evolving third-party data market.

Sincerely,

## Frank A. Marnell

Senior Legal Counsel | *Division of Insurance*

South Dakota Department of Labor and Regulation

Tel: 605.773.3563 | 124 S Euclid Ave ▪ Pierre | [dlr.sd.gov/insurance](http://dlr.sd.gov/insurance)



Confidentiality Notice: This e-mail is intended only for the person(s) to which it is addressed and may contain information that is privileged, confidential, or otherwise protected from disclosure. Dissemination, distribution or copying of this e-mail or the information herein by anyone other than the intended recipient, or an employee or agent responsible for delivering the message to the intended recipient, is prohibited. If you have received this e-mail in error, please advise sender by e-mail at [Frank.Marnell@state.sd.us](mailto:Frank.Marnell@state.sd.us) and delete the e-mail from your server or computer. Thank you.

**From:** Chapman, Randi <Randi.Chapman@bcbsa.com>  
**Sent:** Thursday, September 19, 2024 10:47 AM  
**To:** Alexander, Lois <LAlexander@naic.org>  
**Cc:** Weyhenmeyer, Erica <Erica.Weyhenmeyer@illinois.gov>  
**Subject:** BCBSA comments on draft privacy model exposure

**CAUTION:** This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hello Lois,

BCBSA appreciates for the opportunity to provide feedback on the portion of the Chair's Draft privacy model exposed for comment. Please see our brief comments below. We look forward to continued work with the PPWG as this model development process moves along.

Please do not hesitate to contact me if you have any questions or need any additional information or resources.

With best regards,

Randi Chapman  
202 826 5156

- *In Section 5(A), to closer align with HIPAA and its definition of a third-party, we recommend striking “Consistent with the size and complexity of the third-party” and replace with “A licensee other than a licensee that is a Covered Entity as defined in HIPAA”.*
- *The language in Section 5(A)(4) obligates the third party to share copies of their contracts with their subcontractors with the licensee. However, contracts between third parties and their subcontractors are confidential. They are prohibited from sharing the contracts. We recommend NAIC remove the reference.*
- *In Section 5(A)(6) the language obligates the third-party to notify the licensee of a breach within 48 hours. We recommend including language to reflect the possibility that notification within 48 hours of a breach may be infeasible and that it should be a reasonable time upon discovery.*



**John Euwema**  
VP-Legislative/Regulatory Counsel  
1300 Pennsylvania Ave, NW 190-327  
Washington, DC 20004  
630.824.7300

---

September 18, 2024

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

C/O: Lois Alexander, NAIC Market Regulation Manager  
Sent by email: [lalexander@naic.org](mailto:lalexander@naic.org) and [privacywg@naic.org](mailto:privacywg@naic.org)

Re: Comments to NAIC Privacy Protections Working Group Chair Draft of Amendments to Model Act #672

Dear Working Group Chair Amy Beard, Vice Chair Erica Weyhenmeyer, and Working Group Members,

Thank you for the opportunity to provide comments to Chair Draft Article II, Section 5 – Third Party Arrangements. We hope that our comments and suggested language prove helpful and constructive to the Working Group’s deliberations to craft a privacy protection regime that protects consumers’ personal information balanced with legitimate and important business practices and needs.

Section A

We suggest that the opening paragraph also note that the third party contract may be constructed not just to the complexity of the arrangement but also to the purpose of the arrangement and the information that may be collected.

Section A (2)

Third party service providers who provide anti-fraud services or OFAC compliance may be required to retain certain information, allowance of which should be reflected in revising the Section to include at the Section end “...of the third party or licensee”.

---

CCIA is a national trade association comprised of insurers, providers, administrators and distributors of optional consumer asset and credit protection products such as credit insurance, debt protection, lender placed insurance, AD&D, guaranteed asset protection, service contracts and motor clubs.

#### Section A (4)

Requiring a third party to provide their subcontractor agreements to the licensee may be unworkable and unnecessary. These agreements may have terms and conditions that are confidential between those parties which do not impact their obligations to protect the consumers' nonpublic personal information. The obligation of the third party to include in the subcontractor agreements requirements to protect such information should be sufficient for the purpose of this Act.

#### Section A (6)

Section A (6) language appears inconsistent with the requirements for third parties in the Insurance Data Security Model Law (Model Act #668) Section 4(f)(2) "to implement appropriate administrative, technical, and physical measures to protect and secure" nonpublic information. This language could be adopted in lieu of "...to implement and maintain reasonable administrative, technical, and physical data security practices to protect...". State data security laws also may have varying obligations for third party providers to manage and protect nonpublic personal information. For example, the requirement of the third party to provide notice to the licensee of a breach of the integrity of the information within 48 hours may conflict with such laws. We recommend that the Working Group revise this time requirement to "...within 48 hours or such time frame consistent with other applicable state laws".

#### Section B

There may be factual situations where the licensee should not be solely responsible for data integrity and compliance with this Act which bears further evaluation. Further, the term "data integrity" requires definition to adequately describe the duty imposed upon the licensee.

Finally, we note that "personal information" appears used in Section 5 and elsewhere in the Act in place of "non-public personal information".

Thank you again for the opportunity to comment and for the collegial efforts of the Working Group.

Respectfully submitted,

