

September 20th, 2021

NAIC Privacy Protections (D) 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

Dear Chair Amann, Vice Chair Kreiter and Members of the Privacy Protections Working Group:

Thank you very much for the continued opportunity to provide comments on your ongoing review of past and current consumer privacy frameworks. We very much appreciate the extensive work that the NAIC Privacy Protections Working Group is doing to develop their Privacy Policy Statement. ACLI appreciates this opportunity to participate in the process, as our members are deeply engaged.

As mentioned in our July remarks, we are proud of the fact that the insurance industry has long been a consumer privacy leader in adhering to clear obligations in the appropriate collection, use, and sharing of personal information. Keeping our policyholders' personal information private and protected is at the core of what we do. Life insurers believe it is important for consumers to have certain rights with respect to personal information that companies maintain about them. At the same time, companies need the ability to maintain and process such personal information to provide consumers with the products and services they request, as well as to ensure the accuracy and integrity of information they use and to comply with applicable laws and regulations.

Insurers have ably managed consumers' sensitive medical and financial data for well over a century. The collection and use of personal information is essential to our core business functions – for example, to underwrite applications for new insurance policies, to pay claims submitted under these policies, and to provide longevity protection through retirement products.

Given the sensitivity of the data that insurers collect from and about consumers, insurers are currently subject to several comprehensive federal and state privacy laws and regulations. Our industry's commitment to appropriate use and safeguarding of consumer information has helped establish what has become a thorough federal and state regulatory framework governing the use and disclosure of personal information for the insurance industry. These requirements provide a complex, broad, and rigorous structure that requires our industry to protect the privacy, use and security of consumers' personal information. These laws reflect a critically important balance between consumers' legitimate privacy concerns and the proper use of personal information to serve existing and prospective consumers. And while we recognize and support the need for

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.

modernization of these laws given advances in technology and the expanding use of personal information, we believe that harmonization with existing laws and simplification should be core precepts in developing a national data privacy standard.

We offer the following thoughts on the “Opt-In” provisions of the Privacy Policy Statement.

Opt-In

Life insurers support the reasonable ability for consumers to have control over their personal information. We agree that certain situations should seek an opt-in to share sensitive personal information with third parties. However, we respectfully disagree with the blanket recommendation that all personal information held by insurers and insurance support organizations only be used on the basis of express (opt-in) consent.

Unlike certain business entities where consumer data is essentially the product, insurers provide essential insurance, financial and retirement products, services, and advice to consumers. Insurers need to disclose certain personal information not only to offer consumers options from which they may select appropriate products to fit their unique individual needs, but also for a wide variety of essential insurance, business, and regulatory-required purposes, many of which require the assistance of contracted third parties to perform services on insurers’ behalf and restrict other uses or disclosures by those third parties. As noted, insurers have been subject to comprehensive federal and state privacy laws and regulations for decades - laws which continue to enable an essential balance between consumers’ growing demand for convenience and personalized service and their valid privacy concerns about the collection, use, and sharing of their personal information.

The fundamental nature of the business of insurance requires carriers to collect highly sensitive personal information for the purpose of evaluating risks. Moreover, consumers authorize and opt-in to the collection of this information. As required by current financial services privacy rules and insurance law, consumers receive notice of information practices and a notice of privacy policy as well provide explicit consent to the collection of personal information when they apply for an insurance product. In insurance transactions, the consumer often initiates the transaction and personally provides much of the information needed.

As reflected in the current NAIC Privacy Models #672 and #670, Gramm-Leach-Bliley Act, HIPAA, and other privacy frameworks, the sensitivity of the personal information must be considered in determining whether consent is necessary, and if it is, which form of consent to use (implied or express) or a higher form of authorization. Express consent could be appropriate when: 1) the personal information collected, used or disclosed is sensitive; 2) the collection, use and disclosure would be beyond an individual’s reasonable expectation; or 3) the collection, use and disclosure would pose a residual risk of significant harm to the individual. Those same laws and privacy frameworks recognize that exceptions are necessary and permissible for certain purposes. Sections 15, 16, and 17 of existing Model Regulation #672 reflect important exceptions when personal information needs to be disclosed or shared by insurers with contracted service providers, for processing and servicing transactions, and for other legally-required purposes such as anti-money laundering and fraud reporting. With respect to sensitive health information, the exceptions described in Section 18 of that Model should be preserved: claims administration; claims adjustment and management; detection, investigation or reporting of actual or potential fraud, misrepresentation or criminal activity; underwriting; policy placement or issuance; loss control; ratemaking and guaranty fund functions; reinsurance and excess loss insurance; risk

management; case management; disease management; quality assurance; quality improvement; performance evaluation; provider credentialing verification; utilization review; peer review activities; actuarial, scientific, medical or public policy research; grievance procedures; internal administration of compliance, managerial, and information systems; policyholder service functions; auditing; reporting; database security; administration of consumer disputes and inquiries; external accreditation standards; the replacement of a group benefit plan or workers compensation policy or program; activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit; any activity that permits disclosure without authorization pursuant to HIPAA; disclosure that is required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out a transaction or providing a product or service that a consumer requests or authorizes; and any activity otherwise permitted by law, required pursuant to governmental reporting authority, or to comply with legal process. Similarly, in limited circumstances, the HIPAA Privacy Rule permits covered entities to disclose Protected Health Information to third parties without an individual's opt-in consent or authorization for activities referred to as treatment, payment and healthcare operations (TPO). This would include many of the purposes mentioned above such as quality assurance and utilization review. An important consideration the Working Group should keep in mind is the effect an opt-in consent model will have on the critical ability of insurers to disclose certain information to insurance producers and reinsurers.

Opt-in provisions would also potentially prevent businesses from deriving or inferring data from any set of personal data. Insurers comingle data to ensure that the information is accurate and correct and for such consumer beneficial practices such as pre-population of information on an application. Opt-in should not be required for any expected, contextual internal use.

If a company is only permitted to collect, use, and share data strictly necessary to provide a good or service requested, the ability to expand access to affordable financial security protection and learning in underserved communities, develop joint marketing programs with other financial institutions to benefit consumers, and develop new products will be severely impeded. This ultimately harms consumers by hampering the industry's ability to better serve them. Companies can provide consumer privacy, including providing consumers with rights to control their data, without these dramatic limitations.

We believe the concerns expressed about the use or sharing of certain personal information for targeted advertising are not unique to the insurance industry and would caution against a recommendation that treated insurers and their consumers differently than other financial institutions or businesses in general. With respect to modern advertising and digital marketing, it may be helpful for the Working Group to review and better understand the different and innovative ways that it is accomplished without the use of personally identifiable information. Self-regulatory ad industry bodies such as The Data & Marketing Association (formerly the Direct Marketing Association), The Association of National Advertisers, and The Interactive Advertising Bureau develop and enforce standards and principles that advertisers are expected to adhere to and offer choices to consumers to stop tracking or limit targeted advertising such as the [AdChoices opt-out mechanism](#). The Working Group are likely aware that most browsers and mobile app platforms already provide or require user-level settings and options be available to enable consumers to opt-in or change their personal preferences with respect to cookies, tags, and other tracking signals used for advertising and related analytics purposes. Industry studies show that consumers appreciate relevant advertisements, but do not want invasive tracking or surveillance. For those reasons, there are significant changes occurring within the tech and advertising industries in response to moves by tech companies. Such moves include Apple's introduction of

its app tracking transparency (ATT) framework, and Google's plans to block use of third-party cookies in its popular Chrome browser.

Consumers today expect and appreciate when insurers can anticipate and suggest ways to meet their unique insurance and financial needs, provide personalized customer service, offer custom advice, learning and product recommendations, remember their preferences, and streamline their interactions and transactions to make them easier, simpler, and more convenient. That high degree of personalization may likely not be possible if every element required a consumer or existing customer to check multiple boxes or repeat tasks at multiple, frequent intervals to opt-in every time sharing of certain personal information was necessary with contracted services providers and partners. Instead, it would lead to frustration, "consent fatigue", and complaints. Such an approach would be untenable.

A Balanced Approach

Our members support a balanced, risk-based privacy framework that appropriately assesses risk and operational challenges with consumer protection. No one specific mechanism for consumer control is suitable in all instances. Organizations should be permitted flexibility in how these controls may reasonably be exercised in light of the sensitivity of the personal information. Where organizations rely upon "consent" to collect and use personal information, the type of consent required should be contextual, considering the nature of both the personal information and its proposed uses.

We note that the NAIC Insurance Information and Privacy Protection Model Act (Model #670) and the NAIC Privacy of Consumer Financial and Health Information Regulation (Model #672) have thus far been sufficient to protect consumers for decades, and that even more restrictive frameworks like GDPR do not rely alone on consent to share personal information.

Insurers, like banks and other financial institutions are subject to the Gramm-Leach-Bliley Act (GLBA) which limits them from selling or sharing consumer or customer personal information with third-parties for the latter's own marketing purposes unless certain conditions are met including providing them with notice of their practices and the ability to easily exercise their right to opt-out of such sharing before it occurs. Under the GLBA, insurers must inform consumers about data-sharing practices and explain to consumers their rights if they do not want their information shared with certain third parties. The NAIC Model #672, the state insurance mechanism for GLBA implementation, requires companies to inform consumers if the company intends to disclose nonpublic personal financial information to third parties outside of specific exceptions. Moreover, companies must let the consumer know that they have the right to opt-out of that disclosure, and to provide a reasonable means by which the consumer may exercise the opt-out right. The regulation provides examples of adequate notice as well as reasonable opt-out means, including an electronic opt-out option.

Insurers value their relationships with consumers and their families, many of which are ongoing for years or decades. To avoid jeopardizing those long-term relationships and to avoid increased reputational risk or risk losing control by allowing third parties to market their own products or services to consumers, most insurers do not "sell" consumers' personal information outright to third parties. Where permitted, they may enter into joint marketing relationships with other financial institutions in order to jointly market relevant products and services to benefit consumers – not to exploit them.


GLBA, and subsequently NAIC Model #672, provide a carefully curated list of exceptions to opt-out such as with the consent, or at the direction, of the consumer or to protect confidentiality or security of the information or to protect against fraud, among other reasons. These exceptions provide a useful starting point for the kinds of personal information companies must share to provide and service consumer insurance products. Similarly, the Fair Credit Reporting Act (“FCRA”) provides consumer protections for the sharing of personal financial information provided to financial services companies by consumer reporting agencies. FCRA requires insurers to notify consumers if they plan to share information with affiliates and provide an opportunity for the consumer to opt-out.

Privacy laws applicable to insurers should continue to reinforce these balanced, tested consumer expectations by maintaining an opt-out framework rooted in GLBA going forward.

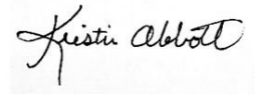
Conclusion

Thank you for your consideration of our comments. ACLI looks forward to continuing to engage with the Working Group throughout this process.

Sincerely,



Shelby Schoensee
Associate Counsel



Kristin Abbott
Counsel