Date: 12/4/21 Version 3

2021 Fall National Meeting
San Diego, California

PRIVACY PROTECTIONS (D) WORKING GROUP
Saturday, December 11, 2021
1:00 – 2:00 p.m.
Convention Center—Room 29—Upper Level

ROLL CALL

Cynthia Amann, Chair	Missouri	Martin Swanson	Nebraska
Ron Kreiter, Vice Chair	Kentucky	Chris Aufenthie/ Johnny Palsgraaf	North Dakota
Damon Diederich	California		
Erica Weyhenmeyer	Illinois	Teresa Green	Oklahoma
LeAnn Crow	Kansas	Raven Collins/Brian Fordham	Oregon
T.J. Patton	Minnesota	Gary Jones	Pennsylvania
Molly Plummer	Montana	Katie Johnson	Virginia

NAIC Support Staff: Lois E. Alexander

AGENDA

1. Consider Adoption of its Nov. 22, Oct. 25, and Oct. 11 Minutes —*Cynthia Amann (MO)* — Attachments 1-3
2. Receive Comments on the Final Exposure Draft of the Privacy Protections (D) Working Group Report on Consumer Data Privacy Protections—*Cynthia Amann (MO)* — Attachments 4-13
3. Consider Adoption of the Final Exposure Draft of the Privacy Protections (D) Working Group Report on Consumer Data Privacy Protections—*Cynthia Amann (MO)* — Attachments 14-15
4. Discuss Any Other Matters Brought Before the Working Group —*Cynthia Amann (MO)*
5. Adjournment—*Cynthia Amann (MO)*

Attachment XX
Market Regulation and Consumer Affairs (D) Committee
12/15/21

Draft: 12/3/21

Privacy Protections (D) Working Group
Virtual Meeting
October 11, 2021

The Privacy Protections (D) Working Group of the Market Regulation and Consumer Affairs (D) Committee met Oct. 11, 2021. The following Working Group members participated: Cynthia Amann, Chair (MO); Ron Kreiter, Vice Chair (KY); Damon Diederich (CA); LeAnn Crow (KS); Chris Aufenthie (ND); Teresa Green (OK); and Don Beatty (VA). Also participating were: Giovanni Muzzarelli (CA); Scott Woods (FL); Tate Flott and Brenda Johnson (KS); Robert Wake (ME); Jo LeDuc (MO); Hermoliva Abejar (NV); Mary Block (VT); Barbara Belling, Darcy Paskey, and Mark Prodoehl (WI).

1. Adopted its Sept. 27, Sept. 13, and Aug. 30 Minutes

Ms. Amann said the Working Group met Sept. 27, Sept. 13, and Aug. 30 and took the following action: 1) adopted its July 12 minutes; 2) heard an update from the NAIC Summer National Meeting; 3) heard updates on federal and state legislative activity by NAIC Legal staff; 4) heard an update on California Proposition 24 by Mr. Diederich; 5) exposed the first exposure draft of the Privacy Policy Statement; 6) received additional comments from a consumer perspective by NAIC consumer representative Harry Ting (Healthcare Consumer Advocate); and 7) received comments on Segment One – Right to Opt-Out of Data Privacy and Segment Two – Right to Opt-In to Data Privacy from the American Council of Life Insurers (ACLI), the Coalition of Health Carriers, the American Property Casualty Insurance Association (APCIA), the Medical Professional Liability (MPL) Association, and NAIC consumer representatives Brenda J. Cude (University of Georgia) and Karrol Kitt (University of Texas at Austin).

Mr. Kreiter made a motion, seconded by Mr. Beatty, to adopt the Working Group's Sept. 27 (Attachment XX), Sept. 13 (Attachment XX), and Aug. 30 (Attachment XX) minutes. The motion passed unanimously.

2. Received a Legislative Update from NAIC Staff

Brooke Stringer (NAIC) said activity in the privacy arena was picking up with the U.S. Senate (Senate) Committee on Commerce, Science, and Transportation having hearings with a former Federal Trade Commission (FTC) official testifying on behalf of the effort. She said Chairwoman Maria Cantwell (D-WA) was also pushing for the creation and funding of a new privacy and data enforcement agency. She said a recent *Wall Street Journal* article distributed to Working Group members and interested state insurance regulators indicated that the FTC has been supportive of privacy regulation by states as well. Ms. Stringer said a group of democratic senators had also called upon the FTC to begin rulemaking with ranking member Senator Roger Wicker (R-MS) wanting the U.S. Congress (Congress) to do it instead to avoid business confusion and strengthen online privacy disclosures. Ms. Amann asked if any drafting had begun. Ms. Stringer said there had been some proposals, but no compromise ones yet. She also said the Senate Committee on Commerce, Science, and Transportation wants to find a consensus.

Jennifer McAdam (NAIC) said there had also been some state legislative activity with work on regulations for the California Consumer Privacy Act (CCPA) currently and the California Consumer Rights Act (CCRA) later; passage by Colorado and Virginia as well as the Uniform Laws Commission (ULC); legislation pending in Ohio; and House Bill 2968 proposed in Oklahoma on computer data. She said state legislatures will meet next in February 2022; however, she said most states will begin preparations in December 2021 and January 2022. She said updated state legislative charts would be posted soon.

3. Received Comments on Segment Three of the Exposure Draft

Ms. Amann said written comments were received on Segment Three from the ACLI, the Coalition of Health Carriers, and Dr. Ting. She said comments received by the deadline are posted to the Working Group's web page. She said comments received after the deadline would be posted soon. She said all comments received would be considered by the Working Group for incorporation into the exposure draft as it goes through the segments to complete its charges. She said the discussion at this meeting would be on comments received on Segment Three – Right to Request Correction of Data, as addressed in pages 32–36.

Kristin Abbott (ACLI) said her comments are on behalf of Shelby Schoensee (ACLI) as well. Ms. Abbott said ACLI members

support the reasonable ability for consumers to request that inaccurate personal information be amended or corrected and challenge such requests based upon the nature, source, or use of the information. She said this important consumer protection principle is one the insurance industry has long supported under existing laws and regulations that remain highly relevant today, such as the *NAIC Insurance Information and Privacy Protection Model Act* (#670), the Fair Credit Reporting Act (FCRA), and the Health Insurance Portability and Accountability Act of 1996's (HIPAA's) Right to Request an Amendment of Protected Health Information. She said these same principles should also apply to newer forms and sources of personal information because insurers understand the critical importance of data integrity and that it be kept accurate and up to date where necessary and as soon as reasonably possible, subject to certain conditions and verification. She said ACLI members share the Working Group's commitment to consumer protection but request that the Working Group keep in mind the importance of context as recommendations are considered. She said it is one thing for an insurer to agree to update out-of-date contact information such as a mailing address, email address, or telephone number, or a change in name or demographic status. She said it is another thing for an insurance customer or claimant to request an alteration or change in personal information collected and relied upon for risk evaluation and decision-making regarding underwriting, the extent of coverage, or claims. She asked the Working Group to consider the underwriting process and where information is obtained directly from the individual or from third parties. She said in instances where the information is obtained from an individual, it is important to allow for a correction or amendment when information is validated as having been incorrectly transcribed or otherwise inputted into an insurance company's underwriting process. She said in instances where information is obtained from a third party, such as their attending physician, an insurance company is not the appropriate entity to make a correction to the underlying information. She said those documents are controlled by the physician, and correction and/or amendment requests should be directed to the physician rather than the insurer. She said if the physician does not make such a change, then Model #670 contemplates adding a statement to the policy file indicating this dispute. She also said new technologies, including artificial intelligence (AI) or AI-enabled systems are revolutionizing and benefitting nearly all aspects of society and the economy. She said given the significant ethical and technical challenges and risks that extend far beyond the U.S. insurance industry and continue to challenge many stakeholders, the ACLI hopes that the Working Group will avoid prematurely making overly prescriptive recommendations regarding the Right to Correct Personal Information that deviate from the existing privacy laws and regulations that insurers continue to abide by. Ms. Schoensee asked if consumers are positive as to their rights to information and/or correction.

Chris Petersen (Arbor Strategies LLC), speaking on behalf of the Coalition of Health Carriers, said use of the phrase, "the right to request" is inaccurate because what should be discussed is the process on how to exercise a request and what companies need to do, which is already covered in Model #670 and HIPAA. He said the Coalition of Health Carriers would like more precise definitions to be used, such as those included in its comment letter. He said word processing is needed, not regulation. He said the issue is data security versus data privacy, which is about the uses and disclosure of information. He said good data security means all data is locked up. He said record retention is generally set by state statute. He said consumers should never have an absolute right to correct data. He said much of the data used must be kept for criminal investigations and similar legally required situations, so consumers should be able to request data but not the right to correct it, which is stated in Model #670, HIPAA, and the FCRA. He said consumers should want the source of the inaccurate data to fix whatever is incorrect, not the insurance companies. Angela Gleason (APCIA) said she agrees with the ACLI and the Coalition of Health Carriers because they have the best interests of consumers in mind, but it seems consumers would like sources to correct data for all requesters. Cate Paolino (National Association of Mutual Insurance Companies—NAMIC) said there are two primary themes: 1) the nature of roles and relationships that industry helps consumers navigate as fiduciaries; and 2) the importance of details, which should be meaningful; therefore, she recommends that no significant changes or revisions to the models are needed, nor is any new model.

Ms. Abejar said the right to delete should adhere to statutory retention requirements. Dr. Ting said companies need to minimize the data collected to only what is absolutely necessary to provide the insurance coverage purchased so there would be less data for companies to control. He also said personal data should never be sold. He said data breaches occur even at organizations with tight security because data can be locked up, but it can also be hacked, so he would support deleting consumer data as soon as the underwriting decision has been made.

Birny Birnbaum (Center for Economic Justice—CEJ) said Dr. Ting is talking about data that is no longer needed while Mr. Peterson is talking about record retention. Ms. Kitt said the timeline for record retention varies by state, type, and purpose. Mr. Birnbaum said life insurers have to keep data longer due to the nature of their business. Ms. Kitt said such data should be put into a silent area like a black box so it can be pulled if it is needed, but it should also prevent the company's marketing unit from seeing it. Mr. Wake said it is a privacy issue, except for specified purposes. Mr. Birnbaum said regarding the right to correct, he opposes the ACLI and the Coalition of Health Carriers' position because it would mean that consumers would have the responsibility to track down and correct any inaccurate data. He said insurers should have to correct it, and they should have to refer consumers to third-party users to make such changes. He said consumers should have an absolute right to view,

access, correct, and delete their data regardless of what the FCRA and HIPAA say. He said the requirement to investigate is anti-consumer when referring to a third party. He also said the key under HIPAA is that the industry is saying they have no responsibility over their third-party affiliates' data. He said the FCRA dispute model directs consumers to go to the furnisher of information to research and correct the data, as well as correct the credit reporting agencies.

Ms. Amann said she is hesitant to set a timeline for the completion of changes to the models, but she is okay with setting best practices for companies that indicate how long a company needs to keep underwriting information used for declination. When asked if there is a need to keep it at all, she said state market conduct examiners would need to be able to document the reason for a company's declination during a market conduct examination many years after the declination occurs. Mr. Wake said there is a legal requirement to lock data for examinations, audits, arbitrations, litigation, record retention, and dispute situations. He said we have the technology to do so. Ms. Amann said the model would have to include this expectation. She said an FCRA requirement is that a letter of protest from a consumer must be kept by the insurer, and it must be sent with any future requests for data. She said she would put various parameters of these issues about the business practices of insurers in writing, and she would put forth data to correct but not change for edits but not comments.

Ms. Amann said during the next call on Oct. 25, the Working Group will discuss comments received by Oct. 18 on Segment Four – Right to Correct Information, as addressed in pages 36–39. She said the following schedule was posted to the web page:

- Comments received by Nov. 1 on Segment Five – Right of Data Portability, as addressed in pages 39–46, would be discussed at the Nov. 8 meeting.
- Comments received by Nov. 15 on Segment Six – Right to Restrict the Use of Data, as addressed in pages 46–50, would be discussed at the Nov. 22 meeting.

Having no further business, the Privacy Protections (D) Working Group adjourned.

W:\National Meetings\2021\Fall\Cmte\D\Privacy Protections\Oct 11\Privacyprot_101121_Min.Docx

Attachment XX
Market Regulation and Consumer Affairs (D) Committee
--/--/21

Draft: 12/4/21

Privacy Protections (D) Working Group
Virtual Meeting
October 25, 2021

The Privacy Protections (D) Working Group of the Market Regulation and Consumer Affairs (D) Committee met Oct. 25, 2021. The following Working Group members participated: Ron Kreiter, Vice Chair (KY); Sam Singh (CA); Erica Weyhenmeyer (IL); LeAnn Crow (KS); Chris Aufenthie (ND); Teresa Green (OK); Scott D. Martin (OR); and Gary Jones (PA).

1. Received a Legislative Update from NAIC Staff

Brooke Stringer (NAIC) said as mentioned during its Oct. 11 meeting, the Working Group is starting to see an uptick in federal interest on data privacy again. She said the U.S. Senate Committee on Commerce, Science, and Transportation held a series of hearings on protecting consumer privacy. Ms. Stringer said Committee Chair Maria Cantwell supports a comprehensive federal privacy law that provides clear protections for consumers, articulates specific limits and obligations of companies, and grants the Federal Trade Commission (FTC) the resources and explicit authority necessary to enforce the new law; however, specifics about preemption and private right of action are still unresolved. She said since the U.S. Congress has not moved substantially on data privacy, the FTC is considering writing rules to strengthen online privacy protections to circumvent the congressional logjams. Ms. Stringer said the rules under consideration could impose significant new obligations on businesses across the economy related to how they handle consumer data. She said the FTC released a report to Congress in September that highlighted its priorities for future data security and privacy protection efforts and urged Congress to allocate more resources to the agency so it could expand its data security and privacy protections efforts. Ms. Stringer said the FTC report link is: *https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf*.

Going forward, Ms. Stringer said the FTC intends to focus its data security and privacy protection efforts on four key initiatives: 1) integrating competition concerns; 2) advancing remedies; 3) focusing on digital platforms; and 4) expanding the understanding of algorithms. Ms. Stringer said the FTC will develop a greater understanding of algorithms, as well as the consumer protection and competitive risks they may pose. She said the FTC will also provide more in-depth guidance for businesses on using algorithms and artificial intelligence (AI) fairly and equitably. In particular, she said the FTC would like to understand the ways that algorithms may create racial bias and work to prevent such uses of algorithms. Ms. Stringer said the FTC will also act to encourage companies to comply with its previously issued recommendation that companies "test their algorithms, both at the outset and periodically thereafter, to make sure it doesn't create a disparate impact on a protected class."

2. Received Comments on Segment Four of the Exposure Draft

Mr. Kreiter said written comments were received on Segment Four from the American Council of Life Insurers (ACLI) and NAIC consumer representative Karrol Kitt (The University of Texas at Austin). He said comments received by the deadline are posted to the Working Group's web page. Mr. Kreiter said comments received after the deadline would be posted soon. He said all comments received would be considered by the Working Group for incorporation into the exposure draft as it goes through the segments to complete its charges. Mr. Kreiter said the discussion at this meeting would be on comments received on Segment Four—the right to delete data.

Shelby Schoensee (ACLI) said on behalf of herself and Kristin Abbott (ACLI), this week recognizes consumers' legitimate interest in requesting deletion of personal information. She said the ACLI is committed to maintaining the integrity of the information used to provide products and services to consumers. Ms. Schoensee said the *NAIC Insurance Information and Privacy Protection Model Act* (#670) currently provides consumers with robust rights to correct, amend, or delete personal information while still recognizing that insurance companies may deny those requests when retention is legally, or practically, required. She said that exceptions to the right to deletion should be clear to consumers so they understand that maintaining data regarding consumers' contracts may include many decades and that such data may become subject to litigation for years in the future. Ms. Schoensee said the ACLI supports the approach of existing frameworks, which acknowledge those realities and provide appropriate exceptions. She said the need for insurers to retain customer and personal information in order to comply with such rules, administer policies, and pay claims is critical. Ms. Schoensee

said the ACLI supports reasonable laws and regulations and giving consumers the ability to request deletion. She said the ACLI also believes that the necessary exceptions should be clear and consistent for consumers. She said the ACLI recommends that existing models and several already-enacted state privacy laws should be relied upon in developing a comprehensive list of exceptions.

Ms. Kitt said individual consumers need to have access to the information that is being collected on them so they can make any corrections that may be needed if something is misstated. She said she is also a strong supporter of the consumer's right to be forgotten—that is, to have any data collected on them to not be held indefinitely by companies. Ms. Kitt said once the use for the data has been completed, such as for underwriting new coverage or paying a claim, then the consumer should have the right to request that the data in question be considered forgotten by the company. She said the data should be held in a private section apart from that available for current use. While in this holding area, she said the data should not be sold, reviewed, or accessed for any other purpose. Once the relationship with the insurer ceases to exist due to a policy cancellation or change to another carrier, the data should be deleted completely, unless it needs to be held for legal purposes. In any case, the data should not be actively used by the company for any purpose once the relationship ends.

Chris Petersen (Arbor Strategies LLC), speaking on behalf of the Coalition of Health Carriers, said Ms. Kitt, Bonnie Burns (California Healthcare Advocates), and Birny Birnbaum (Center for Economic Justice—CEJ) have raised some additional consumer rights and issues that have not yet been addressed by this Working Group. He said they are correct in that some of these rights assume a right to access. Mr. Petersen said he was under the impression that the Working Group identified six of the more contentious issues or the six issues that are not uniform. He said the right to receive a privacy notice is a statutory right that is not in this discussion, but he did not think the Working Group was talking about getting rid of that. He asked if the six rights in this framework paper were supposed to be the only rights given; the most contentious ones; or something else. Mr. Petersen said Arbor Strategies' recommendation is for the right to delete to be included with the right to correct as it is included that way in the models and other legislation currently. However, he said that it should not be an absolute right as he had previously stated. Mr. Petersen said no action had been taken by the Working Group on his recommendations or on those of other interested parties. He said that there needs to be clear definitions developed for each of these rights as they are rather vague currently. He also recommended that the *Privacy of Consumer Financial and Health Information Regulation* (#672) be the focus of this group as it already includes privacy notice and consent disclosure requirements, as well as the federal Health Insurance Portability Accessibility Act (HIPAA).

Ms. Burns said she wanted to reinforce what Ms. Kitt said about some of the contacts that she has with consumers. She said that she does a lot of research online that involves health insurance in one form or another and that she consistently gets advertising for all kinds of health products from agents and agencies selling insurance even though she has blockers designed to prevent the selling of her data on her browser.

Mr. Birnbaum said the requirements for companies maintaining data for purposes unrelated to an ongoing business relationship should be distinguished from companies maintaining data and using it for ongoing business purposes. He said it is fine for a company to maintain a consumer's data if a company no longer has an active ongoing relationship with the consumer and is maintaining data to comply with either data maintenance requirements or other requirements, but he said it is another thing to use the data that the company is maintaining. Mr. Birnbaum said compliance with the law should not be seen as an open opportunity to continue to use those data for purposes for which the consumer has not agreed. He said the other two points would be the right to delete presumes that a customer has knowledge of the data collected by an insurer and how it is used. However, massive amounts of data are collected by insurers that do not require consent by the consumer, such as research collection, and the uses of most data are obscure to most consumers. Mr. Birnbaum said any consumer right to delete data must require that the consumer has knowledge about the data that is being collected and how it is being used. He said the right to delete also presumes that there is a usable and responsive mechanism that exists for consumers to perform such deletion. Mr. Birnbaum said deletion mechanisms can be completely defeated by overly expansive terms and conditions of online agreements or by overly expansive or obscure privacy policies. So, he said that he mentioned all of this so that the right to delete is not viewed as something that is set off by itself, but that it is tightly integrated with all of the other consumer data requirements and consumer privacy protections.

Following up on a couple of Mr. Petersen's comments, Mr. Birnbaum said with health insurance being subject to HIPAA, it has more responsibilities than property/casualty (P/C) insurers and even life insurance. He said what may be a required

notice for health insurers or requirement for health insurance is not necessarily the same requirement for life insurance, or for P/C insurers. Mr. Birnbaum said the right to a notice and a consent to collect and use tends to be limited by the federal *Fair Credit Reporting Act*, which does not apply to a lot of the new sorts of data that insurers are now collecting. He said when talking about opt in or opt out, the presumption is that there is an opportunity for consent disclosure and consent that does not necessarily exist. Mr. Birnbaum said it certainly does no't exist on the property category side for things like social media or web browsing data that are not subject to the requirements of credit reporting yet. He said the Working Group needs to think about the current models in light of the new types of data that are available and the limitations of existing frameworks to reach some new types of data.

Mr. Kreiter said Mr. Birnbaum is correct that some of the items Ms. Stringer presented on the federal level are going to filter down to things that the Working Group will need to consider.

Cate Paolino (National Association of Mutual Insurance Companies—NAMIC) said as the Working Group goes through the rights, some of them have begun to blend together. For example, some of the things the Working Group is talking about may ultimately not relate to deletion, such as things that need to be done for maintaining information for regulatory purposes or for compliance purposes. Things that are spelled out in Model #670 and listed in NAMIC's letter may change when the facts of case litigation occur years later. She said this is less about the deletion of the record and more about something other than that. To reiterate, Ms. Paolino said Model #670 contains many of the provisions and a reasonable way to frame up the right to deletion in terms of how it dovetails with some of the other things.

Mr. Kreiter said the Working Group was tasked with analyzing and determining how these six privacy rights are being protected. He said because of the change in certain federal statutes, the Working Group is trying to work on shifting ground. However, he said the Working Group will continue accepting comments and obtaining ideas to determine if the Working Group can develop a report of recommendations to the Market Regulation and Consumer Affairs (D) Committee that the Working Group can agree upon. When Mr. Petersen asked when the report or determinations would be made, Mr. Kreiter said he did not have an exact date, but said he thinks it would be coming together soon so a final draft of the report could be exposed for a public comment period and edits prior to the Fall National Meeting. He asked Lois E. Alexander (NAIC) if that was her understanding. Ms. Alexander said that the Working Group had been charged with analyzing federal and state legislation, as well as the current NAIC models. She said the six rights that were handed down by the members to the Working Group as a privacy strategy also needed to be reviewed. Ms. Alexander said the Working Group was charged with making recommendations regarding possible revisions to the existing models or the creation of a new model if necessary. She said these recommendations, as Mr. Kreiter noted, will be presented with the Working Group's report with its privacy policy statement to the Market Regulation and Consumer Affairs (D) Committee at the Fall National Meeting. When Mr. Petersen asked if those recommendations would be considered and voted on in a public meeting, Ms. Alexander said they would. Mr. Petersen said the Working Group had not discussed any of the issues yet. However, Ms. Alexander said the Working Group has been discussing these issues since December 2019, when the initial work plan was introduced. Since that time, the public discussions have been ongoing, with everyone having an opportunity to discuss other pertinent aspects of consumer data privacy rights as they were developed. She said the Working Group will discuss the last two privacy rights on their Nov. 22 call and that the Working Group will add them in the Working Group's report to its parent committee.

Mr. Kreiter said during its next meeting on Nov. 8, the Working Group will discuss comments received by Oct. 25 on Segment Five—the right of data portability, as addressed in Pages 39–46.

Having no further business, the Privacy Protections (D) Working Group adjourned.

MinutesGuide.docx

Attachment XX
Market Regulation and Consumer Affairs (D) Committee
--/--/21

Draft: 12/5/21

Privacy Protections (D) Working Group
Virtual Meeting
November 22, 2021

The Privacy Protections (D) Working Group of the Market Regulation and Consumer Affairs (D) Committee met Nov. 22, 2021. The following Working Group members participated: Cynthia Amann, Chair (MO); Ron Kreiter, Vice Chair (KY); Damon Diederich and Sam Singh (CA); Erica Weyhenmeyer (IL); LeAnn Crow, Tate Flott, and Shannon Lloyd (KS); T.J. Patton (MN); Molly Plummer (MT); Chris Aufenthie and Janelle Middlestead (ND); Gary Jones (PA); and Katie Johnson and Don Beatty (VA). Also participating were Kurt Swan (CT); Jan Davis (FL); Robert A. Wake (ME); Marjorie Thompson (MO); and Shelley Wiseman (UT).

1. Received a Legislative Update from NAIC Staff

Brooke Stringer (NAIC) said legislation had been drafted on both sides of the aisle, but there is nothing substantive yet.

Jennifer McAdam (NAIC) said there had been no activity as state legislatures will not meet again until Feb. 2022. However, she said most states will begin preparations in December and January.

2. Received Comments on Segment Five and Segment Six of the Privacy Policy Statement Exposure Draft

Ms. Amann said written comments were received on Segment Five—The Right to Data Portability and Segment Six—The Right to Restrict the Use of Data from the American Council of Life Insurers (ACLI) and on Segment Five from the Coalition of Health Carriers. She said comments received by the deadline are posted to the Working Group's web page. Ms. Amann said comments received after the deadline would be posted soon. She said all comments received would be considered by the Working Group for incorporation into the exposure draft as it goes through the segments to complete its charges. She said the discussion at this meeting would be on comments received on Segment Five and Segment Six.

Kristin Abbott (ACLI) said her comments are on behalf of Shelby Schoensee (ACLI) as well. Ms. Abbott said ACLI members support a consumer's right to request a copy of certain personal identifiable information (PII) and to provide that requested information in a usable format requested by the consumer, if technically feasible. She said given the lack of demand or any direct practical benefit to consumers, ACLI members were concerned with the cost and significant security risks in trying to accommodate such requests. Ms. Abbott asked that the Working Group consider the unintended and disruptive consequences of offering consumers an indefinite, absolute right to restrict all uses of their personal information or only to certain uses specified by the consumer. She said ACLI members appreciate the work the Working Group is doing and look forward to continuing this conversation in relation to the latest exposure draft. Ms. Amann said she appreciates the comments made and that she is picking up some of the more consistent thoughts from various interested parties, so she asked interested parties not to think that their comments have been ignored. She said everyone's comments will be in the draft eventually. However, some may not show up until version two or seven or 12. Karrol Kitt (The University of Texas at Austin) asked Ms. Abbott if she was referring to the fact that there is little demand for the portability of consumer data or if there is little benefit. She asked if the ACLI could substantiate how consumer demand is related to consumer knowledge. Ms. Kitt said since there is no historical data collection, there needs to be a new understanding and new disclosures to build consumer knowledge as it relates to such consumer data privacy issues due to the new technical insurance environment.

Ms. Amann said the existing models did not contemplate the current environment, so the models need to be revised, but to what extent and whether revised disclosures are the answer has yet to be determined. She said historically consumers have not been aware or knowledgeable about such issues. However, she said this will be a major focus for the Working Group in 2022. Birny Birnbaum (Center for Economic Justice—CEJ) said consumers are seen as commodities by industry; those insurers can get to purchase or use their products by limiting consumers' choices via algorithms. However, he said to consumer advocates, consumers are persons who need to know what choices are available to them. Mr. Birnbaum said consumers should have access to their own health information like they have access to their financial information so they can share either with those the consumer chooses.

Chris Petersen (Arbor Strategies LLC), speaking on behalf of the Coalition of Health Carriers, asked how federal Health Insurance Portability Accessibility Act (HIPAA) requirements would allow insurers to share a consumer's data as it is specifically prohibited. He said the individual consumers would have to request their own data and then share it with other entities themselves. He said financial institutions could share consumers' information with their consent. Mr. Petersen said there are different sets of rules for financial and health concerns. He said the Working Group takes a term and treats it differently

from the way it is generally known (e.g., within the General Data Protection Regulation [GDPR]). Mr. Petersen said the Working Group should not use the term "portability" as it is defined in the GDPR, but rather the Working Group needs to define "portability" differently or use the term "access." He said the Working Group should also look at the *NAIC Insurance Information and Privacy Protection Model Act* (#670) and HIPAA. Mr. Birnbaum said that would be inappropriate because the GDPR allows entities to destroy data. Mr. Wake said HIPAA mandated a data standardization regime. Mr. Diederich said insurers need to disclose this information via authorizations. Mr. Petersen said the term "portability" is not used in the insurance industry. Ms. Schoensee said that this is a complicated issue but that all participants have the same goal, which is to find a balance between insurers and consumers. She said there needs to be additional, meaningful, and thoughtful consideration before the Working Group can move on to an exposure draft. Ms. Amann said there will be more robust discussions and definitions to come and while the Working Group is revising the NAIC models in 2022. She said the Working Group welcomes everyone's input as it develops a succinct draft of revisions needed. Wes Bissett (Independent Insurance Agents & Brokers of America—IIABA) asked when data ownership and potential public policies were added to the rights discussed by the Working Group. Ms. Amann said the Working Group has noted during almost every meeting that right is being used with a lowercase "r" to reflect that it is not an absolute right, but more like a category for discussion. She said the right of consumer data ownership was informally added to the Working Group's discussions during the Innovation and Technology (EX) Task Force at the Summer National Meeting.

Mr. Bissett said he appreciates the review of privacy laws, but he is concerned with the policy statement in Appendix A. He said the privacy policy statement in Appendix A was not discussed previously within the Working Group meetings. Mr. Bissett said he is concerned that in the paper, it refers to a right of data ownership as though it is some sort of already existing inalienable right. He said there are references to it sort of being a minimum consumer privacy protection that should apply in the business of insurance. So, Mr. Bissett said asked, "Has the Working Group already made the decision, so we are now at the point where there ought to be a requirement related to data portability? What is going to happen next? Is it that the existing models will be revised so that they reflect the existence of this?" Ms. Amann said that is not the case. She said the right of data ownership was not included when the Working Group started down the road on their charges. However, at the Summer National Meeting, the Working Group was given the authority to add data ownership as one of the rights being reviewed. Ms. Amann said the Working Group is talking about rights with a lowercase "r" and not as in an inalienable right as Mr. Bissett mentioned. She said data ownership is an issue that will be fought over going forward. She said the Working Group has not made a definitive statement on it but rather put it in as a placeholder to be discussed more in the future. Mr. Bissett said maybe the paper needs to make clearer that these are potential public policy outcomes that are being discussed; that they are all on the table' and that no decisions have been made yet. He said the suggestion or implication appeared to be in the paper right now and that the Working Group appeared to have concluded that if there is not a right to something like data portability, then there ought to be such a right, and that the models were going to be revised to provide those rights.

Ms. Amann said if that is what people are seeing, the Working Group need to correct it because that is not the intention. She said the Working Group has identified certain rights, but the Working Group has not made any decisions about all consumers needing to have these 10 topics or rights. Ms. Amann said these rights are areas of concern that state insurance regulators and consumer representatives have pertaining to the privacy of consumer data, so the Working Group does not want to get hung up on the word "right" at this time. She said it is a way to say that these are top eight or 10 topics pertaining to privacy and privacy protections that the Working Group wanted to address. Lois E. Alexander (NAIC) reminded everyone that the Working Group received the strategic initiative from NAIC members in April regarding privacy wherein the members identified these issues as "rights," so the Working Group has used that term because it is the term used by NAIC members in their directive passed on through the parent committee. Mr. Bissett said the term is still a source of ongoing confusion. He said even if one looks at these as potential requirements that would apply to industry, some industry folks at least wonder where these came from. Mr. Bissett said in the paper, there is a reference that insurance licensees should provide a periodic notice of its privacy policies and practices not less than annually. He said he does not remember the meeting where that was discussed, or if there was a vote taken on that, which flies in the face of what state and federal regulators have done in recent years on that.

Ms. Amann said going forward, these are the types of issues that may warrant regulatory requirement, regulatory input, or some sort of oversight because of the impact upon the consumer. So, she said while it is not the intent of this report, those types of issues could become the topics for discussion going forward. However, she said the Working Group is not there right now and is not making any kind of regulatory requirements in this policy statement. Ms. Amann said if language comes across that way, the Working Group can make some refinements to it for clarification. She said that she appreciates the comments and said sometimes the only way one can tell if something that was written hit the mark is to say it out loud and to hear others give an impression of how they are taking it. Ms. Alexander said to clarify, what is in the paper that Mr. Bissett is talking about is just a summary of discussions of selected topic; it is not cast in stone.

Mr. Bissett said his chief concern and that of others in the industry is with Appendix A, which seems to be almost like a mini model law of its own or a series of recommendations. He said that is where he saw the recommendation that there ought to be

no less than an annual privacy notice requirement and it talks about a specific timing of 30 days. He said this seems to be a specific public policy requirement or recommendation that has not been talked about. Mr. Bissett said perhaps there should be further conversation about whether there needs to be access to and obligations put on licensees or certain types of licensees. He said it seems like the hand is being put on the scale with specific recommendations that are being made in the appendix and based on this assumption, industry's recommendation at this point would be to remove Appendix A altogether or at least to continue discussions. Ms. Amann said an undercurrent to the whole issue is that Model #672 long at 77 pages, so it needs a great deal of streamlining to make clear what is expected, what someone can or cannot request, and what someone can or cannot do. She said one of the problems with the whole privacy issue is that there are a lot of requirements already and maybe the requirements are not stated as clearly as possible. Or, she said maybe consumers do not act as they should with how business has evolved now as compared to when these models were initially drafted. Mr. Bissett said he thinks it would be a helpful tool for industry, regulators, and policymakers if a state is interested in a particular issue, that the provision of a model law where that is addressed would link up issues as to how these issues are addressed in other NAIC models.

Mr. Birnbaum said the charge to the Working Group is to review problems in protections and make recommended changes as needed to certain models. He said what Mr. Bissett is saying is that the Working Group should remove any recommendations. However, if the Working Group did that, it would not be carrying out its charge. He said the Working Group is making recommendations. It is not making law, and that is exactly what the Working Group is charged with doing. Mr. Bissett said those recommendations had not been discussed. Mr. Birnbaum said the recommendations had been discussed in this Working Group. Mr. Wake said one thing Mr. Bissett might be trying to say is that some of the existing provisions should be removed or streamlined because the things Mr. Bissett was concerned about are taken straight out of existing models. Mr. Wake said it might be fair to say that as the Working Group considers how to strengthen the models, it might also look at what the models are currently doing that could be done better in some other form next year.

Mr. Diederich said much of what is in the policy statement can be found in the existing models, such as the 30-day requirement for disclosure. Mr. Birnbaum said the Working Group is following its charges by making draft recommendations. Mr. Wake said the issues Mr. Bissett has concerns with are already in the models.

Mr. Petersen said the insurance trades, property/casualty (P/C), life, and health met prior to this Working Group meeting to discuss the exposure draft, and they have technical concerns about the definition of "portability" in the paper not being that most commonly used; about opt in being described as an authorization when generally it is used in a state as getting permission to use information for marketing purposes; and that discussions seem to have been occurring in private. He said many of his comments, such as a safe harbor for insurers subject to HIPAA, have been presented in several meetings, but they have not been discussed during any of these meetings. However, he felt the report and policy statement included items that had not been discussed in open meetings. Ms. Amann said there is nothing nefarious going on and that a lot of the writing of the paper was simply to move it along to get an issue put on paper so that the Working Group can make it clear to the Executive (EX) Committee, as well as to the Market Regulation and Consumer Affairs (D) Committee that the Working Group believes that these were chosen as they rise to the level of needing to be addressed better than they are currently in Model# 670 and the *Privacy of Consumer Financial and Health Information Regulation* (#672). She said the Working Group believes that these issues merit attention going forward and that at a minimum, Model #670 and Model #672 need to be updated. She said as far as anything being in the appendix that is trying to set requirements, the Working Group will make sure that it does not. Its sole intention is to draw the reader's attention to areas that the Working Group has concerns with, which is why it is in an appendix, where it reads better when compared to the rest of the paper. She said the technical concerns are a problem because certain terms are used interchangeably, which has also been a problem for other Working Groups working on similar issues. Ms. Amann said they are terms of art, so people who know that read the document a certain way and others who read it interchangeably do not see the distinction, so the Working Group will be mindful of that. She said the Working Group needs to be mindful that it does not use terms incorrectly. Ms. Amann said she does not know if it would increase anyone's comfort level but asked if the reader who has been involved would agree that the Working Group could do that as a minimum. Ms. Amann said the Working Group talked about the safe harbor issue during one meeting, but the Working Group is not ready to go down that road yet because it is not 100% on changes that it believes are needed. She said the Working Group welcomes comments from everyone on the paper to make sure that it is being read correctly.

Mr. Wake said he is surprised to hear that there was a recommendation on portability in the paper, so he looked at the paper again and found that portability data is mentioned. He said portability is one of the issues the Working Group recommended be addressed, but in the appendix, the only recommendation regarding portability is the right of access to one's personal information. Mr. Wake said two-thirds of the states do not have Model #670. He said he imagines that many companies provide the access voluntarily, even in the states that do not mandate it, so that is not really a groundbreaking recommendation in that area. Going beyond that, he said the Working Group needs to think carefully about what the right should be in terms of what opt in means. Mr. Wake said opt in means something affirmative is needed from the consumer before it can be done. In terms of use, it generally does mean disclosure, so he said Mr. Petersen is not wrong, but neither is the paper.

Bob Ridgeway (Blue Cross Blue and Shield Association—BCBSA) asked if the Working Group could move on to the exposure draft. He said Mr. Petersen is correct in that the Working Group had discussed some of the things he wanted to say today and so far, he supports the comments and observations Mr. Petersen made. Mr. Ridgeway said he wants to do some level setting to find out if he is right or not. On Page 13 of the policy statement, there is a paragraph that says, "This policy statement serves the purpose of informing licensed insurance entities, consumers, etc., on what the current models support as the minimum consumer data privacy protections." Mr. Ridgeway said he believes that the core of that sentence is that this is a level-setting document. He said this is where the Working Group is now and that he is not reading it to say any of the issues there are necessarily for further discussion or comment or objection. Mr. Ridgeway said it looks as if it says this is just what is in the models now, what is supported as far as their models, and that is the status quo. He said he is also hearing that this is not the end of the Working Group's tasks, but that the Working Group intends to go on from here and begin to do the true gap analysis that it has discussed during open meetings for a long time, identify specific gaps, and figure out how best to address those gaps as a policy matter. Mr. Ridgeway asked if that is roughly where the paper is now and where the Working Group would be going from here.

Ms. Amann said "yes." She also recognized that there are many nuances to every word used in the paper. Ms. Amann said she is not trying to minimize anyone's concerns, but the paper is about bringing to light certain issues that consumers are having and that state insurance regulators are having where the Working Group believes improvements are needed. She said all this paper is doing is noting the status quo as of right now. Ms. Amann said the intent is not to have the paper say there is no regulatory requirement, but rather that improvements are needed.

Mr. Ridgeway said that is helpful and that he hopes it is to others participating in the meeting. He also said he agrees with Mr. Birnbaum that the Working Group would probably do better going forward to change the verbiage about this "rights" and instead refer to them as potential issues. Ms. Amann said as Ms. Alexander mentioned, "right" was the term given to the Working Group by NAIC membership through the Market Regulation and Consumer Affairs (D) Committee. She said she appreciates the willingness of the Working Group to have the discussion about whether each issue needs to be a right or if it needs to be called something else. Mr. Wake said the Committee also gave the Working Group the charge to a draft a policy statement, and he said that given the state of the deliberations over the last several months, it does not seem right to make any ringing policy statement that goes beyond here are the policies that have been expressed as recommendations to the states and its existing model laws.

Angela Gleason (American Property Casualty Insurance Association—APCIA) said she thinks everyone's concern is with Appendix A and where it is going. Ms. Gleason said she understands that some of it is a statement of existing law, but that the existing laws are complex, so to boil that down into a sentence or two causes a lot of concern. She said all these models are complex, and yet California and Virginia have been able to balance consumer rights and businesses' ability to do business. Ms. Gleason said this issue necessitates some complexity as the concern is that it is hard to boil this down in terms of identifying something as an expectation that there might be a right for the consumer's protection, but there are other pieces that go around that protection. She said that is where industry is coming from, so they appreciate this conversation and will provide some edits that may be more than technical, though.

Mr. Birnbaum said what he hears industry saying is that they want this Working Group to make a variety of policy decisions on behalf of the consumer and that they want those policy decisions to be essentially what industry believes that the policy should be. He said that what the Working Group's charge was is to explore the issues, identify the issues, ask what has been done, and ask what still needs to be done. Mr. Birnbaum said when this policy statement and report go to the parent committee, whether that is the new Innovation, Technology, and Cybersecurity (H) Committee or the Market Regulation and Consumer Affairs (D) Committee, that is where a lot of those policy decisions are going to be made and from where the specific guidance to the Working Group is going to come. So, he said the issues that industry is looking at, such as going line by line through these models, will come later, but first some guidance is needed as to what the Working Group is trying to accomplish. Mr. Birnbaum said he thinks industry is putting the cart before the horse by asking the Working Group to do a lot of stuff when it has been asked to come up with some policy issues first for its parent committee to consider. He said the Working Group is hearing from industry that the Working Group needs to identify problems that industry somehow has not recognized, or is not willing to recognize, and that the Working Group has been looking at that these issues from the beginning. Now industry wants the Working Group to basically throw everything out and start over again. Mr. Birnbaum said what the Working Group is seeing is an industry strategy to basically slow or delay this process of getting a policy paper in front of the policymakers to decide. He said the consumer representatives strongly object to that tactic.

Mr. Ridgeway said he finds Mr. Birnbaum's comments offensive. Mr. Birnbaum said what he finds offensive is industry's portrayal that this Working Group has not identified what the problems are or what the concerns are and that it should start from the beginning again.

Ms. Gleason said that she is not saying the Working Group should start from the beginning; she is saying she does not necessarily understand an example of where the problem is because industry is not getting complaints from consumers. She said she understands that this issue been pushed back on industry by saying maybe consumers do not know what to complain about or who to complain to, but she said she had not heard anything other than identifying what the issues are. Ms. Gleason said each side is showing their position, and the Working Group has not had a conversation about it until now. She said she understands that is another step, but she is not in any way telling this Working Group to start over. Ms. Gleason said she is just asking for some understanding because industry does not understand what the issues are.

Ms. Amann said she can see where this misunderstanding could have happened because the Working Group started down a certain road with the templates for each of the rights under which it was going to try to give a little bit more detail. She said the decision was made to do the policy statement because consumer representatives brought their information and wanted to give the Working Group assistance on this issue. With many other points of view, Ms. Amann said the intent was that the policy statement would be a good road map to follow when the Working Group moved into the modifications of the models. She said the Working Group has concluded that Model #670 and Model #672 need fixing, so that is where the Working Group is going. Ms. Amann said the Working Group will report this recommendation to the Market Regulation and Consumer Affairs (D) Committee at the Fall National Meeting in this format with any necessary corrections addressed. She said if there is something in the report or policy statement that makes it sound like there is a conclusion or that there is a regulatory recommendation, that is not the intent right now. Ms. Amann said the report will not have the 15 examples per right that the Working Group initially started collecting because the report and policy statement are at a much higher level

Bonnie Burns (California Health Advocates) said this is a new area for her and that she would like to weigh in with total support of Mr. Birnbaum's position. She said one of the things that she had not heard discussed during this meeting that she is concerned about is what companies do with the data that they have, whether companies tailor information sent to consumers based on the data that they have, or whether companies withhold some of the information. Based on the data that companies have, Ms. Burns said she has concerns about how the data is used beyond what Mr. Birnbaum and the rest of the Working Group and industry have been talking about. Ms. Amann said she knows that is one of the charges for the Innovation, Technology, and Cybersecurity (H) Committee for 2022 is to delve into more of the data collection, data usage, and all that interplay. She said to the extent that consumer data, privacy protection, and that overlap, the Working Group will address that going forward, but for purposes of the paper for this policy statement, the Working Group just has a short little instruction to fulfill. Ms. Burns said she can tell everyone from her own experience that consumers know there is a lot of data held by companies, but they have no idea what that data is or how they can do anything about it. She said knowledge about how what data companies have or how they use it is not available to consumers, so the fact that consumers have not submitted a lot of complaints is not surprising. Mr. Petersen said Ms. Burns is suggesting that other than the notices that companies send out on a regular basis on health insurance, that companies also tell people that they have this information and how they use it. He said this way, the right to access would be that consumers have the right to change it, which is what he has heard consumer representatives say. Mr. Petersen said the context is what more the Working Group can do other than inform people through notices that were prescribed in those notices by law. Ms. Burns said for one thing, those consumer notices had not been tested because consumers do not understand them and do not realize what they are supposed to do with them. Mr. Petersen said the federal government dictates the language companies must use in the required notices. Harry Ting (Health Care Consumer Advocate) asked if the health information collected on consumers is gathered using cookies. If so, he asked if cookies and other data scanning online software is covered by HIPPA because if it is not, then consumers generally do not understand that it is being collected and that it could be harmful. Mr. Ting said it is important that consumers be able to observe what data cookies and online scanning are obtaining if that is being used. Mr. Petersen asked Mr. Ting if this question is about who is collecting that information because some of the examples that have been used during this meeting are not about health insurance carriers collecting the data. Mr. Ting said that is exactly why he asked because such notices are probably not required for health insurance carriers. Mr. Petersen said to the extent that consumers go online and use some sort of research system to try to find health insurance coverage, one could be making their personal data available to outside third parties, which may not even be covered by insurance laws. Mr. Ting said the insurers should be held responsible if they are working with certain organizations to obtain data, then insurers should make the consumer data privacy notice a requirement of the organizations that they are getting the data from. He said he understands that enforcement might be difficult, but that could be part of a requirement that would be added to the regulation.

Ms. Amann said those would be the types of issues the Working Group would have to flush out next year when looking at Model #670 and Model #672 because she guarantees that the models did not include the word "cookies" or any of the Insurtech terms or practices. She said to the extent that the Working Group wants to ensure that the models are applicable to Insurtech, the Working Group would have to include any licensed third-party administrator (TPA) or other entity to ensure that those models overtly state who is covered and who is not, which will take a great deal of drafting. Mr. Ridgeway said if the consumer hit the covered entity or health insurer, each has information on a consumer and shares that with some other entity, then they must issue a notice to the consumer. He said they can only do so if that other entity becomes what is known as a business

associate, and they sign documents binding themselves to basically the same requirements that HIPPA imposes on the health insurer. Mr. Ridgeway said on the other hand, if this is somebody who reveals information on the Internet or somehow an individual who does that is one of the Working Group's concerns, that at least has increasingly been when data becomes easily transferable by the consumer from one entity to the other. The consumers probably do not have much recollection or realization that when they are turning their information loose on the Internet, it is gone, there is no telling who is going to get it, and there is no way consumers can pull it back out.

Mr. Ting said he is a volunteer Senior Health Insurance Information Program (SHIIP) counselor, so he counsels people dealing with Medicare. He said he had an individual last month who was covered by a Medicare supplement policy that she had been under for 10 years. He said she was happy with it, but she got a cold call from an agent who wanted to switch her to a different plan. She told the agent that she was not interested. Without her knowledge, she got a letter from the insurance company that she had previously saying that effective next month, she would no longer be on their plan. Mr. Ting said he had to call Medicare to find out what happened. Mr. Ting said he found out that this person had her information and switched the policy by sharing her data without notice or her agreement. So, he said there are situations where people are unethically doing this, but when he talks to individuals and he thinks they are understanding, it is not clear whether they are covered by HIPAA because companies are using this data inappropriately and harming innocent people. Mr. Ting said that is an example of something where he would like to see that there are adequate rules that should help to protect seniors and other vulnerable populations against situations where those kinds of unethical practices occur. Mr. Ridgeway said this type of situation is covered under agent licensing laws. He said if the agent who did that was, in fact, a licensed agent and has not been reported to his or her state insurance regulator, the agent should be. Ms. Amann said this is a good conversation to have going forward so that the Working Group can ensure that if it does need to refer something to another Working Group, it can. She said she welcomes having examples brought up if it helps identify a gap.

Cate Paolino (National Association of Mutual Insurance Companies—NAMIC) said she had a few items, and they probably run more to the procedural for now. She said the email that accompanied the exposure draft had requested feedback to find minor edits. She said so many things come to mind because there is so much to look at that her comments may be more substantial than minor edits. Ms. Amann said to look at the policy statement as a road map with placeholders where areas to be discussed reside, and then provide comments in the form of bullet points (in the interest of time) marking areas of concern or where something may need to be added. She asked that they not be read as written, but more as a thought put out in front of the parent committee to let it know that there are many issues that need to be reviewed. Ms. Amann said it is a higher level than a white paper would be because a white paper does eventually come to conclusions, so this is more of a good recommendation or a good area for the Working Group to delve into further. She said she recognizes the Working Group will go through the Model #670 and Model #672 line by line, but she does want the Working Group to have a better idea now of the areas that need consumer protection or regulatory oversight of company practices because to make sure that the models are as succinct as they can be. Ms. Amann said that the Working Group does want to just wordsmith it, but rather wants to change them to reflect actual practices that are occurring. She said the Working Group should think of it as a little bit more than an outline, but a lot less than a white paper.

Ms. Paolino asked whether there might be any flexibility regarding the deadline. Ms. Amann said the Working Group must be able to get comments in, compile them into some sort of format, then work with Ms. Alexander to draft something into the report. Ms. Amann said while she is not opposed to another day or two, the Working Group needs the comments quickly. She said they do not have to be formal—just bullet points or a simple statement. That was one of the initial reasons to back up and start over with a more high-level approach, so the Working Group could give everyone an idea of where it is going and what areas it feels have the most need for consumer protection or the most need for regulatory responsibility,

Erica Eversman (Automotive Association) said consumers do not seem to have any problems entering personal or intimate data online into Twitter or Facebook. However, as it relates to consumers not knowing or consumers not making comments, complaints, or concerns about data collection or their access to data, she reiterated what Ms. Burns and Mr. Ting were saying in that the consumers she deals with have absolutely no idea how insurance operates. She said they do not know how insurance decisions are determined, how their premiums are determined, or that there are departments of insurance (DOIs) to whom they can reach out to for help. Ms. Eversman said consumers do not know how any of this works, so they would never have any idea that they could make a complaint or request information about themselves from their insurer. Ms. Abbott said she would like to echo the concerns raised by industry representatives today and that ACLI members have many similar concerns, especially in relation to the appendix, and that they really appreciate the clarification. Randi Chapman (BCBSA) said she wants to echo the comments that her colleagues across the industry trades have made and to thank all of them for speaking up. She also said she appreciates the additional clarity provided during this meeting. She asked if it is possible to extend the comment deadline to Dec. 6. Ms. Amann said she will discuss it with the Working Group vice chair and NAIC staff and will send an email with a decision about timing for comments.

Mr. Ting suggested an edit on Appendix A. He said right now, it is a policy statement on consumer data privacy protections. If it were changed to a policy statement on consumer data privacy protection issues, that might clarify one thing and then in the paragraph or two where different subject areas were introduced, the Working Group could say that these are areas that have been identified for examination to see if there are any improvements needed. Mr. Birnbaum asked if the principals for artificial intelligence (AI) represent an example of a policy statement by the NAIC. Ms. Amann said "yes." Mr. Ting said his research on personal information ownership indicates there is a broad consensus across the board that there is no established legal basis for saying that anyone has full ownership of the data that the Working Group is talking about. He said there are certain circumstances where that data can be used, even if the person does not want it to be used, such as where there are legal issues involving fraud or other types of issues if there are national security issues and so forth, so his sense is that basically there is no legal basis to say that any consumer has full ownership or full control over the data. He said what that really means is the Working Group needs to look at each of the issues as it is evolving. How is such data being used? What kind of data can people collect? What kind of data can people share? How can they share it? Mr. Ting said that is really the basis on which the Working Group must look at data ownership rather than saying that someone owns it entirely.

Ms. Amann said she will discuss this with Mr. Kreiter and Ms. Alexander. Then she will get an email out with some reminders. She said the intent is to receive comments by Dec. 2 because the Working Group has a national meeting to get ready for. She said another document that was done at a high level was the paper on accelerated underwriting, and it touches on some of these issues—at least tangentially. So, that is another document to read to get thoughts on where state insurance regulators are coming from that the Working Group hopes to get moved up at the Fall National Meeting.

Ms. Amann said at the Fall National Meeting, the Working Group will discuss comments received by Dec. 2 on the final exposure draft of the report to the Market Regulation and Consumer Affairs (D) Committee. She reminded the Working Group members that they need to register for the Fall National Meeting to participate and that those attending the Working Group meeting virtually will be able to participate by audio only. Ms. Amann said there will not be cameras, but the sound is usually good, so they can hear everybody speak.

Having no further business, the Privacy Protections (D) Working Group adjourned.

Attmt 3_PPWG_112221 Minutes

CMA: combined suggested changes from Consumer Reps, ACLI and Trades/Joint Group

Privacy Protections (D) Working Group Report on Consumer Data Privacy Protections

Exposure Draft

December 7, 2021

Table of Contents

I. Introduction

The Privacy Protections (D) Working Group was appointed in 2019 to review state insurance privacy protections regarding the collection, use, and disclosure of information gathered in connection with insurance transactions and make recommended changes, as needed, to NAIC models addressing privacy protection. This work included the review of an insurer's use of data collected from a consumer and data supplied to an insurer by a third-party vendor. Rather than focusing on revisions to NAIC models, the main deliverables for 2021 were to set forth a Report on the minimum consumer privacy protections that are appropriate for the business of insurance, after taking into consideration the consumer privacy protections that already exist under applicable state and federal laws.

The Working Group discussed how best to balance the need for information by those conducting the business of insurance and the consumer's need for fairness in insurance information practices. ~~rights of insurers to use data for legitimate business purposes with consumers' rights to control what data is used and how it is used.~~ The following privacy protections for consumers were discussed: (1) the right to opt out of data sharing, (2) the right to limit data sharing unless the consumer opts in, (3) the right to correct information, (4) the right to delete information, (5) the right of data portability, (6) the right to restrict the use of data, (7) the right of data ownership, (8) the right of notice, and (9) the right of nondiscrimination and/or non-retaliation.

As a reminder, opting in is not a way the consumer can protect their privacy – it is a way a consumer can waive a privacy protection. The Working Group intended to consolidate (1) and (2) above as a single "right to restrict data sharing, on either an opt-out or an opt-in basis," however, since these issues were discussed extensively as separate "rights" that for purposes of this Report the issues are being listed separately.

The Working Group received comments from the ACLI, AHIP, APCIA, BCBSA, the Coalition of Health Insurers, NAMIC, MLPA, and NAIC consumer representatives Birny Birnbaum, Brenda Cude, Karrol Kitt, and Harry Ting.

II. Overview of Issue

Consumer awareness and regulatory concerns about the use of consumer data by a variety of commercial, financial, and technology companies are increasing. This has led to the adoption of the General Data Protection Regulation (GDPR) in the E.U. and the California Consumer Privacy Act (CCPA) and other state data privacy protection laws in the U.S. Though data privacy concerns extend beyond the insurance sector, the increasing use of data and the passage of these new laws is causing the insurance industry and consumer groups alike to compel Congress to enact federal privacy legislation.

While federal legislative efforts are currently stalled due to other legislative priorities and differing perspectives from consumers and industry on the best path forward, it is likely that Congress will begin focusing on the issue again soon. The current pause provides state insurance regulators an opportunity to update state privacy protections consistent with the current insurance business environment and potentially forestall or mitigate the impacts of any preemptive federal legislation. State policymakers have also responded to the privacy debate with varying legislative proposals to provide consumers with greater transparency and control over the use of personal information, with California, Virginia, and Colorado being the most recent examples. These comprehensive state data privacy laws each have either entity-level or data-level exemptions for entities subject to or information collected pursuant to the federal Gramm-Leach-Bliley Act (GLBA) and/or the privacy regulations adopted under the Health Insurance Portability and Accountability Act (HIPAA).

III. Summary of Consumer Privacy Protections Provided by NAIC Model Laws

The NAIC has three model laws governing data privacy: *Health Information Privacy Model Act* (Model #55); *NAIC Insurance Information and Privacy Protection Model Act* (#670) and *Privacy of Consumer Financial and Health Information Regulation* (#672), each of which is based upon or influenced by federal privacy laws. The NAIC's Model #670 contains many of the consumer rights found in these comprehensive state laws, which can be traced back to the Fair Credit Reporting Act (FCRA), and Model #672 is based, in large part, on GLBA and the HIPAA regulations. Generally, insurers and other entities licensed by state departments of insurance have certain exemptions from ~~are carved out of~~ more comprehensive state laws of general applicability.

Because of thee exemptions, insurance regulators must be aware when new protections are added to laws applicable to other businesses, especially when these laws address new technologies and ways consumer information is collected and shared, so that comparable protection can be added, as necessary, to the laws governing the insurance industry. Of note, GLBA and HIPAA each set a federal floor for the entities within their scope, upon which states can build. This is what the NAIC did in drafting the *Health Information Privacy Model Act* (Model #55) and the *Privacy of Consumer Financial and Health Information Regulation* (Model #672). GLBA applies to the entire insurance industry while HIPAA applies to the health insurance sector and those that collect or use Protected Health Information {PHI}.

A. NAIC Insurance Information and Privacy Protection Model Act (Model #670)

The NAIC adopted the *NAIC Insurance Information and Privacy Protection Model Act* (#670) in 1980 following federal enactment of the Fair Credit Reporting Act in 1970 and the Federal Privacy Act in 1974. This model act establishes standards for the collection, use and disclosure of information gathered in connection with insurance transactions by insurance companies, insurance producers and insurance support organizations.

A key aspect of this model is that it establishes a regulatory framework for consumers to: (1) ascertain what information is being or has been collected about them in connection with insurance transactions; (2) obtain access to such information for the purpose of verifying or disputing its accuracy; (3) limit the disclosure of information collected in connection with insurance transactions; and (4) obtain the reasons for any adverse underwriting decision.

This regulatory framework is facilitated through a requirement that insurers or agents provide a written notice to all applicants and policyholders regarding the insurer's information practices. The notice must address the following: (1) whether personal information may be collected from persons other than the individual or individuals seeking insurance coverage; (2) the types of personal information that may be collected, the types of sources and investigative techniques that may be used to collect such information; (3) the types of disclosures allowed under the law; (4) a description of the rights established under the law; and (5) notice that information obtained from a report prepared by an insurance support organization may be retained by the insurance support organization and disclosed to other persons.

Of note, the model prohibits disclosure of any personal information about an individual collected or received in connection with an insurance transaction without the individual's written authorization, subject to limited exceptions. However, some categories of information may be disclosed for marketing purposes if the consumer "has been given an opportunity to indicate that he or she does not want personal information disclosed for marketing purposes and has given no indication that he or she does not want the information disclosed." Model #670 also provides consumers with the right to request that an insurer provide access to recorded personal information, disclose the identity of the third parties to whom the insurance company disclosed information (if recorded); disclose the source of collected information (if available); and provide procedures by which the consumer may request correction, amendment, or deletion of recorded personal information.

Seventeen (17) states have adopted Model #670: AZ, CA, CT, GA, HI, IL, KS, MA, ME, MN, MT, NV, NJ, NC, OH, OR, and VA.

B. NAIC Health Information Privacy Model Act (Model #55)

The NAIC adopted the *Health Information Privacy Model Act* (Model #55) following federal adoption of the privacy regulations authorized by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

This model sets standards to protect health information from unauthorized collection, use and disclosure by requiring insurance companies to establish procedures for the treatment of all health information by all insurance carriers. The drafters of Model #55 believed it was important that the same rules apply to all lines of insurance, since health insurance carriers are not the only ones that

use health information to transact business. For example, health information is necessary for life insurance underwriting, and often essential to property and casualty insurers in settling workers' compensation claims and personal injury liability claims. Reinsurers also use protected health information write reinsurance.

The model requires carriers to develop and implement written policies, standards, and procedures for the management of health information, including to guard against the unauthorized collection, use or disclosure of protected health information. It provides consumers with the right to access their protected health information and amend any inaccuracies. The model also requires insurers to obtain written authorization ("opt-in") before collecting, using, or disclosing protected health information, except when performing limited activities.

Many of the provisions found in Model #55 were later incorporated into the *Privacy of Consumer Financial and Health Information Regulation* (Model #672).

The following 11 ~~13~~ jurisdictions have adopted legislation related to Model #55: CA, CO, DE, KY, LA, ME, MO, ND, RI, SD, TX.

C. NAIC Privacy of Consumer Financial and Health Information Regulation (Model #672)

The NAIC adopted the *Privacy of Consumer Financial and Health Information Model Regulation (Model #672)* in 2000. The model regulation was drafted to implement the requirements set forth in Title V of GLBA. GLBA imposed privacy and security standards on financial institutions, defined to include insurers and other insurance licensees, and directed state insurance commissioners to adopt certain data privacy and data security regulations. The provisions governing protection of financial information are based on privacy regulations promulgated by federal banking agencies. This model also contains provisions governing protection of health information that were taken directly from Model #55 and from the HIPAA Privacy Rule promulgated by the U.S. Department of Health and Human Services {HHS}.

The model regulation provides protection for non-public financial and personal health information about consumers held by insurance companies, agents, and other entities engaged in insurance activities. In general, the model regulation requires insurers to: (1) notify consumers about their privacy policies; (2) give consumers the opportunity to opt-out of ~~prohibit~~ the sharing of their ~~protected~~ non-public financial information with non-affiliated third parties; and (3) obtain affirmative consent from consumers before sharing ~~protected~~ non-public personal health information with any other parties, affiliates, and non-affiliates.

The key difference between the treatment of financial information and health information is that insurers must give consumers the right to "opt out" of the disclosure or sharing of their financial information but insurers must obtain explicit authorization from the consumer ("opt-in") before sharing health information. Every jurisdiction has a version of this model regulation, although nineteen (19) jurisdictions have only adopted the provisions regarding financial information and not the provisions regarding health information for purposes not within an exemption. Some jurisdictions that have adopted Model #670 have adopted additional provisions from Model #672 by bulletin rather than regulation.

IV. Summary of Health Insurance Portability and Accountability Act (HIPAA)

In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA), which, among other things, authorized the U.S. HHS ~~Department of Health and Human Services~~ to promulgate regulations governing consumer privacy protections. The HIPAA Privacy Rule was finalized in 2000. The rule applies to health plans and health care providers, restricting the permitted uses and disclosure of protected health information. HIPAA preempts state law only to the extent that a covered entity or business associate would find it impossible to comply with both the state and federal requirements.

HIPAA provides individuals the right to (1) access and amend their protected health information, (2) the right to request the restriction of uses and disclosures of protected health information, and (3) the right to receive an accounting of disclosures made to other entities.

A covered entity must obtain the individual's written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care operations or otherwise permitted or required by the law. A covered entity is also required to provide notice of its privacy practices.

V. Summary of General Data Protection Regulation (GDPR)

The GDPR became effective in May 2018 and may apply ~~applies~~ to U.S. companies based on whether or not they process the ~~if they collect~~ data from citizens of the E.U. or are processing data within the E.U. and provided that they have a sufficient nexus with the E.U. ~~over the internet~~. This law requires companies (referred to as data "controllers") to obtain explicit consent from consumers to collect their data ("opt in") along with an explanation of how the data will be used. It also contains standards for safeguarding the data collected. Under the GDPR, a consumer has the following rights: (1) to receive information about the processing of personal data; (2) to obtain access to that personal data; (3) to request that incorrect, inaccurate or incomplete personal data be corrected; (4) to request that personal data be erased when it is no longer needed or if processing it is unlawful; (5) to object to the processing of personal data for marketing purposes or on grounds relating to a consumer's particular situation; (6) to request the restriction of the processing of

personal data in specific cases; (7) to receive personal data in a machine-readable format and the ability to transmit ~~send~~ it to another controller, if technically feasible ("data portability"); and (8) to request that decisions based solely on automated processing concerning the consumer or significantly affecting the consumer and based on a consumer's personal data, are made by human beings or to challenge a decision.

For further clarification - the GDPR does not, necessarily, apply to a company simply because it collects data from citizens of the EU over the internet. Specifically, the company must actively market its products and services to those in the EU. It is a factual determination. For example, routinely shipping goods to the EU, utilizing the French language on the website (in addition to English) and setting a website up to accept euros would likely result in the GDPR applying to a given company.

VI. Summary of Recently Adopted Consumer Privacy Protection Laws

A. California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)

In 2018, California became the first U.S. state to adopt a comprehensive privacy law, applicable beyond the insurance industry, imposing broad obligations on businesses to provide consumers with transparency and control of their personal data. The California Consumer Privacy Act (CCPA) became effective in 2020. Since it was adopted, it was amended by the California Privacy Rights Act (CPRA), which becomes effective January 1, 2023. Additionally, the California Attorney General promulgated implementing regulations in 2020.

Scope

The CCPA, as amended by the CPRA (California law) applies to companies doing business in California that collect or process consumers' personal information and meet one of the following thresholds: (1) has annual gross revenue in excess of $25,000,000 in the preceding calendar year; (2) annually buys, sells, or shares the personal information of 100,000 or more consumers or households; or (3) derives 50% or more of its annual revenue from selling or sharing consumers' personal information.

Exemptions

The law does not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (GLBA), and its implementing regulations. It also does not apply to protected health information that is governed by the privacy, security, and breach notification rules issued by the U.S. ~~Department of Health and Human Services (~~HHS~~)~~. Furthermore, this law contains an entity-level exemption for HIPAA-covered entities or business associates governed by the privacy, security, and breach notification rules issued by HHS.

Consumer Rights

California law provides consumers with the following rights subject to certain limitations: (1) to request deletion of any personal information;[1] (2) to correct inaccurate personal information, taking into account the nature of the personal information and the purposes of the processing of the information; (3) to know about and access the personal information being collected by requesting that the business disclose: the categories and specific pieces of personal information collected, the categories of sources the information was collected from, the business purpose for collecting the information, the categories of third parties with whom the information is shared, and the specific pieces of personal information that was shared; (4) to request the personal information provided by the consumer in a format that is easily understandable, and to the extent technically feasible, in a structured, commonly used, machine-readable format that may also be transmitted to another entity at the consumer's request without hindrance; (5) to know what personal information is sold or shared and to whom; (6) to opt out of the sale or sharing of personal information; (7) to limit the use and disclosure of sensitive personal information aside from permissible enumerated purposes; and (7) to not be retaliated against for requesting to opt out or exercise other rights under the law.

Business Obligations

The law imposes the following obligations on all covered businesses: (1) prohibits retaining a consumer's personal information for longer than reasonably necessary for the disclosed purpose; (2) requires implementing reasonable security procedures and practices; (3) requires notice of the following: collection of personal information, including sensitive personal information, retention of information, right to opt out of sale and sharing, and financial incentives; (4) prohibits using sensitive personal information outside of enumerated purposes when a consumer has requested not to use or disclose such data.

Enforcement

The CPRA amends the CCPA by placing administrative enforcement authority with the California Privacy Protection Agency, a new state agency created by the CPRA. Under the CPRA, the California Attorney General retains authority for seeking injunctions and civil penalties. Additionally, if personal information is breached, the consumer can pursue a private civil action against the company.

[1] And even when information is "deleted," the CCPA right to deletion allows the business to "maintain a confidential record of deletion requests solely for the purpose of preventing the personal information of a consumer who has submitted a deletion request from being sold, for compliance with laws or for other purposes."

B. Colorado Privacy Act (CPA)

Scope

The Colorado Privacy Act (CPA) takes effect on July 1, 2023. Subject to certain limitations this law ~~It~~ applies to entities that conduct business in Colorado or produce or deliver commercial products or services intentionally targeted to residents of Colorado and satisfy one of the following thresholds: (1) controls or processes the personal data of 100,000 or more consumers in a year; or (2) derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of 25,000 or more consumers. The law defines "controllers" as those that "determine the purposes for and means of processing personal data" and defines "processors" as those that "process data on behalf of a controller."

Exemptions

The law contains data-based exemptions (rather than entity-level exemptions) for protected health information collected, processed, or stored by HIPAA-covered entities and their business associates, and information and documents created by a HIPAA-covered entity for purposes of complying with HIPAA and its implementing regulations. Additionally, the law contains an exemption for any personal data collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act (GLBA), and implementing regulations, if such collection, processing, sale, or disclosure is in compliance with that law.

Consumer Rights

The CPA provides consumers with the following rights: (1) to opt out of targeted advertising, sale of personal data, and profiling; (2) to confirm whether a controller is processing the consumer's personal data and the right to access such data; (3) to correct inaccuracies in personal data; (4) to delete personal data; and (5) to obtain the personal data in a portable and readily usable format that allows the consumer to transmit the data to another entity.

Business Obligations

The CPA imposes affirmative obligations on controllers, including the following: (1) provide consumers with an accessible, clear, and meaningful privacy notice; (2) specify the express purposes for which personal data are collected and processed; (3) collection of personal data must be adequate, relevant and limited to what is reasonably necessary in relation to the specified purposes; (4) not process personal data for purposes that are not reasonably necessary to or compatible with the specified purposes, without obtaining consent from the consumer; (5) take reasonable measures to secure personal data; (6) not process personal data in violation of any law that prohibits unlawful discrimination; and (7) not process a consumer's sensitive data without first obtaining the consumer's consent. Additionally, controllers are required to enter into contracts

with data processors, referencing the responsibilities under the CPA and controllers must conduct a data protection assessment prior to any processing activities that have a heightened risk of harm to consumers.

Enforcement

The CPA does not contain a private right of action but does provide the state attorney general and district attorneys authority to take action against entities for violations.

C. Virginia Consumer Data Protection Act (CDPA)

Scope

The Virginia Consumer Data Protection Act (CDPA) becomes effective January 1, 2023. Subject to certain limitations, this law ~~It~~ applies to entities that conduct business in Virginia or produce products or services targeted to Virginia residents when they control or process personal data of at least 100,000 consumers or control or process personal data of at least 25,000 consumers and also derive over 50% of gross revenue from the sale of personal data.

Exemptions

The law contains entity-level exemptions for those subject to GLBA and HIPAA. It specifically exempts financial institutions and data subject to GLBA, and covered entities or business associates governed by the privacy, security, and breach notification rules issued by the U.S. HHS ~~Department of Health and Human Services~~. It also exempts protected health information under HIPAA.

Consumer Rights

The CDPA provides consumers with the following rights: (1) to confirm whether or not a controller is processing the consumer's personal data and if so, to provide the right to access such personal data; (2) to correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of processing of the consumer's personal data; (3) to delete personal data provided by or obtained about the consumer; (4) to obtain a copy of the consumer's personal data in a portable and readily usable format that allows the consumer to transmit the data to another controller; and (5) to opt out of the processing of the personal data for purposes of targeted advertising, sale of personal data, and profiling.

Business Obligations

Under the law, controllers have the responsibility to do the following: (1) limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed; (2) not process personal data without consumer consent for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for

which such personal data is processed; (3) establish, implement, and maintain reasonable data security practices to protect personal data; (4) not process personal data in violation of any laws that prohibit unlawful discrimination against consumers and not discriminate against consumers exercising their rights under this law; and (5) not process sensitive data concerning a consumer without obtaining the consumer's consent. In addition, controllers must provide consumers with a reasonably accessible, clear, and meaningful privacy notice. Processing activities undertaken by a processor on behalf of a controller must be governed by a data processing agreement. Controllers also must conduct data protection assessments that evaluate the risks associated with processing activities.

Enforcement

Similar to the Colorado law, the Virginia law does not contain a private right of action but does provide the state attorney general authority to pursue action against entities for violations.

VII. Summary of Working Group Discussions of Selected Key Points

The Working Group began discussions December 8, 2019, during the Fall National Meeting with the following minimum consumer privacy protections being considered as appropriate for the business of insurance. These rights were based on the Working Group's proposed 2020 charges and are included in the Working Group's initial 2019 Work Plan:

1. the right to receive notice of an insurer's privacy policies and practices;
2. the right to limit an insurer's disclosure of personal data;
3. the right to have access to personal data used by an insurer;
4. the right to request the correction or amendment of personal data used by an insurer;
5. the right of data ownership; and
6. the right of data portability.

An example of the other types of issues the Working Group will need to discuss includes clarifying the specific circumstances for when a "right" does exist. Is it really a "right to request" as contained in the California law? Or is it merely a right to delete inaccurate information like FCRA? Or is it a right to request deletion of inaccurate information as described in Model #670?

Eventually the Working Group decided on nine (9) categories to study. In addition to the six above, the Working Group added (7) the right of data ownership, (8) the right of notice, and (9) the right of nondiscrimination and/or non-retaliation.

The Work Plan also stated that the Working Group discussions would focus on data privacy (and not data security) and identify areas within existing NAIC models and state requirements where consumer data privacy protections might need to be enhanced due to changes in technology. In ~~her~~ a December 8 presentation, Jennifer McAdam (NAIC) outlined existing privacy provisions in

NAIC models and state insurance laws. She said the difference between data privacy and data security is that data privacy is about how data is being collected and used by businesses; while data security is about how data that a business has already collected, has in its possession, and is stored and protected from unauthorized access. She said the two are often conflated and there are some laws that address both – for example, the GDPR.

Furthermore, as many comments have noted, the two issues overlap because a breach of security often results in a loss of privacy. Ms. McAdam said the CCPA is an example of a data privacy law that governs how businesses collect and use consumer data; the rights consumers have to know how that data is being used; the rights consumers have to challenge the accuracy of the data; and how it is being used. Data privacy laws are focused on legal protections for data and consumer rights: In comparison, data security laws, such as the NAIC's Insurance Data Security Model Act (#668), require operational and technological protections sufficient to ensure that the legal protections are meaningful. Ms. McAdam explained that Model #668 governs how businesses protect the data once it has been collected as well as what businesses need to do if those protections fail as the result of a data breach or other cybersecurity event.

The Working Group operated under these distinctions.

State insurance regulators were concerned about the consumer data that insurers were already presenting in rate filings that had ballooned up to thousands of pages of different data points being gathered by insurers on consumers. Regulators have also seen an increased reliance on third-party risk scores that aggregate consumer information in order to make determinations and conclusions about consumer information. Regulators noted that insurers have a responsibility to ensure that the third parties used are following state laws and complying with the state's standards for accuracy and fairness. In addition to providing disclosure of the third parties used by insurers when consumers request it, insurers are required to report how the information was gathered; where it was drawn from (*e.g.*, web traffic, geolocation data, social media, etc.); and why the company thinks it needs to use those particular data points.

Industry asked the Working Group to consider: 1) workability by allowing for various exemptions for operational and other reasons that acknowledge vital business purposes for insurers to collect, use, and disclose information. For example, Article IV of the NAIC Model #672 was developed to implement the GLBA, and the exceptions embedded into Section 13 of Model #672 are instructive as to the types of operational functions that need to be preserved and facilitated; 2) exclusivity by avoiding dual regulation, so insurers are not simultaneously subject to potentially inconsistent or conflicting interpretations by more than one regulator; 3) clarity by asking that care be taken to consider how best to dovetail new requirements with existing models/laws/regulations; consulting other resources and educating legislators on how privacy bill language impacts the insurance industry, including the legal requirements to retain and use certain data, as well as data

mandates; 4) an effective date that allows advance time (like the two to five years that was afforded under the GDPR) for insurers to be ready for implementation, to avoid having piecemeal revisions like the CCPA and the GDPR, as well as a roll-out period with different dates for different provisions within that time frame as a more measured approach to undertake such a significant endeavor.

Consumer Representatives asked the Working Group to consider that: 1) data vendors are scraping personal consumer information from public sources to produce consumer profiles, scores, and other tools for insurers. The data vendor products, while assembled from public information, raise concerns over consumers' digital rights and privacy; 2) many data vendors and many types of personal consumer information are not subject to FCRA consumer protections. In turn, many of the types of data and algorithms used by insurers are not subject to either FCRA consumer protections (even though they are the functional equivalent of a consumer report) or the NAIC model law/regulation protections; 3) it is unclear whether the NAIC models cover the new types of data being generated by consumers as part of, or related to, insurance transactions. For example, consumers are producing large volumes of data through telematics programs from devices collecting personal consumer data in the vehicle or home or through wearable devices; 4) there are several organizations working on consumer digital rights (such as the Center for Digital Democracy, the Electronic Privacy Information Center, the Electronic Frontier Foundation, the Public Knowledge-Privacy Rights Clearinghouse, the Public Citizen, the U.S. Public Interest Research Group, and the World Privacy Forum) from whom input and presentations at Working Group meetings could be solicited; and 5) if consumer disclosures are to be used, that disclosure should be a compliance or enforcement tool that would be created using consumer focus testing and established best practices for the creation of such consumer disclosures.

The COVID-19 pandemic slowed the Working Group's discussions in 2020, however, discussions continued through seven virtual meetings and two regulator-only meetings of subject matter experts as areas of concentration were being narrowed leading to the Working Group receiving additional guidance from its parent committee.

In April 2021, the Working Group's discussions were redirected to six consumer data privacy rights or types of consumer data privacy protections based on the specific examples identified in item 1.c. of the NAIC Member Adopted Strategy for Consumer Data Privacy Protections received through its parent Committee, the Market Regulation and Consumer Affairs (D) Committee. The Working Group's task was to comment on the following consumer privacy rights concerning consumers' personal information as a basis for a privacy protection framework for the insurance industry (not just health insurance):

1. Right to opt out of data sharing;
2. Right to limit data sharing unless the consumer opts in;

3. Right to correct information;
4. Right to delete information;
5. Right to data portability;
6. Right to restrict the use of data.

Consequently, the Working Group was also tasked with analyzing or determining how insurers were protecting these rights – either to comply with state or federal statutory or regulatory requirements, on their own initiative or through the adoption of voluntary standards. In 2021, the Working Group met ten times and the regulator only subject matter experts met nine times.

Prior to the 2021 Summer National Meeting, the Working Group focused on discussion of, and input on, the following key points from regulators, industry, and consumers for each of the six consumer privacy data rights noted above: definitions; examples; consumer risk/impact; current state and federal laws/rules; insurer/licensee impact; actions necessary/insurer obligations to minimize consumer harm; and recommendations. Suggestions that separate privacy requirements be established for each line of business were discussed, but there was consensus that this did not seem to be feasible, as different consumer data privacy requirements across lines of business would limit both consumer protections and understanding.

It was noted during Working Group discussions that insurers are increasingly utilizing third party vendors as sources of data collection and that such vendors may not be subject to regulation by state insurance departments. Regulators stated that the insurers they regulate bear the responsibility for compliance with state insurance privacy requirements. Insurers felt they could not be held responsible because they did not know how such vendors collected or used consumer data and had no way to control the vendors' business activities. Regulators and consumer representatives expressed different opinions indicating that insurers' contracts with such vendors could and should be written to require vendors and insurers maintain compliance with insurance regulations regarding consumer data privacy.

During the 2021 Summer National Meeting, NAIC members further recommended that the Working Group's discussion be expanded to include the issue of consumer data ownership.

Working Group discussions revealed that state insurance regulators and consumer representatives believe consumers own the data that is collected and used by the insurance industry to market, sell, and issue insurance policies. It was felt that the type of data collected (name, age, date of birth, height, weight, income, physical condition, personal habits, etc.) describes who a person is and distinguishes one person from another by its very nature. When a consumer shares their data with an insurance company, it is with the understanding that the consumer is letting the company borrow it for a time to determine what insurance rates and insurance coverage the consumer needs. The consumer is not giving up their data to an insurer so it can be sold or given to other organizations from whom the consumer is not seeking insurance coverage, or any other product. Consumer

representatives indicated that this practice had happened when they did an online search for insurance rates on health plans. As a result, the consumer representative received hundreds of cold calls from companies selling products other than insurance. When the consumer representative asked with whom the insurance company shared his data, the company sent him a list of 1,700 companies – none of which sold insurance. [Trades ask to delete this portion or to make clear that it is opinion and being reported by consumer group but not verified. I do not agree with deleting.]

The Report in Appendix A is designed to be the foundation for the minimum consumer data privacy protections that are appropriate for the business of insurance to be applied to the NAIC models as revisions. It is intended to kick start the next step in creating revisions by defining the parameters of the existing consumer data privacy rights; ~~by suggesting definitions and by showing examples of consumer risks~~ impact. Further discussion is necessary, however, to clarify consumer data privacy rights that may not be fully protected in federal laws or fully covered under NAIC Model laws, and to decide how to provide appropriate protections.

VIII. Conclusion and Recommendations

Months of detailed discussions with regulator, industry, and consumer stakeholders, and the comments they have submitted, have led the Working Group to determine that the *NAIC Insurance Information and Privacy Protection Model Act (Model #670)* and the *Privacy of Consumer Financial and Health Information Regulation (Model #672)* have in the past provided an effective regulatory framework for consumer privacy protections to oversee and enforce consumer data privacy as required by state and federal statutes and regulation. ~~However, these~~ These models were adopted by the NAIC 20 and 40 years ago, respectively; with only 17 jurisdictions adopting Model #670.

However, in consideration of the many business developments and technological improvements that have occurred in recent years, as well as the rate of increase in the use of new technologies (AI, machine learning, accelerated underwriting, rating algorithms, etc.), and big data by insurers, the Working Group recommends additional considerations of the ways that Models #55, #670 and #672 could be amended to ensure that regulators and legislators can continue to have a robust menu of options to provide consumer data privacy protections essential to meet the consumer data privacy challenges presented by the public use of technology and data by insurers in today's business environment.

As a reminder, the standards established in these models, while not only being between 20 and 40 years old, are considered to be a 'floor,' they are basic requirements, and these requirements are not to be considered a 'ceiling' that limits future NAIC initiatives. As business practices and technological developments have progressed so too must the consumer, the industry and the regulator.

It is clear that with the proliferation of data and the use of such data by licensed entities, that insurance regulation needs to modernize to protect the consumer of unintended consequences of the use ownership and security of such data. It is the intention of this Working Group to recommend that either the NAIC models be reopened and revised, or a new Model Law be created concerning the 9 categories listed in this Report, including a focus on data ownership, data rights and data protections. The work product going forward can use the GDPR as a possible template, along with other recently enacted state laws, while keeping in mind federal laws that already protect consumers' data. Emphasis will be given to data transparency, customer control, customer access, data accuracy, and data ownership and portability as explained in Appendix A.

Subsequent to systemic and transparent decisions relating to Appendix A discussions and adoption of any model law changes, the ~~The~~ Working Group also recommends the NAIC's *Market Regulation Handbook* and the NAIC's *IT Examiners' Handbook* be updated, as necessary, to provide guidance to state insurance regulators so they can verify insurers' compliance with the state's regulatory framework for consumer privacy protections.

Appendix A

National Association of Insurance Commissioners
Report on Consumer Data Privacy Protections

By adhering to the same/similar intent behind the drafting of the NAIC's Principles on Artificial Intelligence, this Report also requests that all "… insurance companies and all persons or entities facilitating the business of insurance that play an active role" in the protection of and usage of consumer data … promote, consider, monitor and uphold the principles as described in this Report.

This Report is intended to be a high-level report of the discussions and research conducted by the Privacy Protections (D) Working Group. The focus of our work was determining the minimum consumer data protections that are appropriate for the business of insurance. Once determinations were made, the Working Group discussed whether or not the current model laws are sufficient in order to continue protecting consumers and providing regulatory oversight, are revisions needed or does the Working Group need to draft a new model. This Report can be viewed as being similar to the Ai Principles in that it provides insight to regulatory expectations and serves as an outline for actions to be discussed ~~taken~~ going forward.

This Report only provides research information ~~guidance~~ to the Regulator and does not carry the weight of law or impose any legal liability. This guidance only ~~can serve~~ serves to inform state insurance departments and insurance companies of intended recommendations designed to address improvements needed for data privacy protections and to highlight issues needing further discussion.

Appendix B contains a list of resources relied upon during the pendency of this Working Group.

Because the business operations of insurance companies are dependent upon the collection and use of personal information and data, state insurance regulators have long understood the need to balance an insurance company's need to collect consumer information and data with the consumer's right to understand ~~limit~~ the collection and use of this data.

The NAIC adopted the *Insurance Information and Privacy Protection Model Act* (Model #670) in 1980 to establish standards for the collection, use and disclosure of information gathered in connection with insurance transactions. A key aspect of this model is that it establishes a regulatory framework for consumers to (1) ascertain what information is being or has been collected about them in connection with insurance transactions; (2) obtain access to such information for the purpose of verifying or disputing its accuracy; (3) limit the disclosure of information collected in connection with insurance transactions; and (4) obtain the reasons for any adverse underwriting decision. This regulatory framework is facilitated through a requirement that insurers or agents provide a written notice to all applicants and policyholders regarding the insurer's information practices.

The NAIC adopted the *Privacy of Consumer Financial and Health Information Model Regulation* (Model #672) in 2000. The model regulation was drafted to implement the requirements set forth in Title V of the federal *Gramm-Leach-Bliley Act* (P.L. 106-102) of 1999 (GLBA). GLBA imposed privacy and security standards on financial institutions and directed state insurance commissioners to adopt certain data privacy and data security regulations. The model also contains provisions governing protection of health information that were taken directly from the ~~Health Insurance Portability and Accountability Act (~~HIPAA~~)~~ Privacy Rule promulgated by HHS. The NAIC model regulation requires insurers to: (1) notify consumers about their privacy policies; (2) give consumers the opportunity to ~~prohibit~~ opt-out of the sharing of their ~~protected~~ non-public financial information with non-affiliated third parties; and (3) obtain affirmative consent from consumers before sharing ~~protected~~ non-public personal health information with any other parties, affiliates, and non-affiliates. The key difference between the treatment of financial information and health information is that insurers must give consumers the right (with limited exceptions) to "opt out" of the disclosure or sharing of their non-public financial information to third-parties for the third party's own business use, but insurers must get explicit authorization ("opt in") before sharing health information absent an applicable exception.

This Report addresses consumer data privacy protections of (1) transparency; (2) consumer control; (3) consumer access; (4) data accuracy; and (5) data ownership and portability. The Report intentionally excludes standards for data security and standards for the investigation and notification to an insurance commissioner of a licensed insurance entity's cybersecurity event, ~~which~~ since these issues are the subject of separate model laws and interpretive guidance.

The following definitions are used for the purposes of this policy statement.

A. "Adverse Decision" means declination of insurance coverage, termination of insurance coverage, charging a higher rate for insurance coverage, or denying a claim.
B. "Consumer" means an individual who is seeking to obtain, obtaining, or have obtained a product or service from an insurer. For example, an individual who has submitted an application for insurance is a consumer of the company to which he or she has applied, as is an individual whose policy with the company has expired.
C. "Customer" means a consumer with whom an insurer has an on-going relationship.
   For purposes of this Report, customers are a subset of consumers, so there is no reason to reference "customer or consumer."
D. "Licensee" means any insurer, producer, or other person licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to a state insurance law.
   For purposes of this Report, what is defined above in (D) is a "regulated entity," however, the models have been using the term "licensee" so this Report will continue to use the more

familiar terminology.

E. "Personal Information" means any individually identifiable information or data gathered in connection with an insurance transaction from which judgments can be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit, health, or any other personal characteristics. Personal information includes:

1. "Non-Public Personal Information," which means information that a consumer provides to a licensee to obtain an insurance product or service (like income, credit history, name and address); information about a consumer a licensee has as a result of a transaction involving an insurance product or service (like premium payment history, how much a life insurance policy is worth, and the value of personal property insured); and all other information about a consumer that a licensee uses in connection with providing a product or service to a consumer.
2. "Non-public personal health information," which means any information that identifies a consumer in some way, and includes information about a consumer's health, including past and present physical and mental health, details about health care, and payment for health care.

I. Transparency [Trades have a lot of comments; see ACLI pt 19]

It is recommended that a ~~A~~ licensee ~~should~~ provide a clear and conspicuous notice to consumers that accurately reflects its privacy policies and practices ~~when it first requests personal information about the consumer from the consumer or a third party~~.

It is recommended that a ~~A~~ licensee ~~should also~~ provide a periodic notice of its privacy policies and practices to customers when substantive changes have occurred ~~not less than annually~~ during the continuation of the customer relationship.

If a licensee makes an adverse decision based on information/data that was not supplied by the consumer, it is recommended that the licensee ~~should~~ provide the consumer with the specific reasons for the adverse decision. [Note: this standard is already a requirement – for declinations/nonrenewals the consumer is to be given the reason in such detail as to not require the need for further inquiry. Use Cons Rep example?]

**Going forward the WG types of issues to understand - would ensure all definitions, such as "on-going relationship," consumer and customer are [copasetic]; company business operations are considered, record retention practices are understood, what happens to personal data/info when a person applies for but decides to not purchase a policy; when they cancel the policy; ensure the findings from the gap analysis have been addressed.

II. Consumer Control [Trades – change to Consumer Preference Default Mechanism]

It is recommended that ~~A~~ licensees ~~should~~, at a minimum, provide consumers the opportunity to ~~prohibit~~ limit the sharing of their non-public personal information with third parties, except for specific purposes required or specifically permitted by law. (Opt-Out)

It is recommended that ~~A~~ licensees ~~should~~ obtain affirmative consent from consumers before sharing non-public personal health information with any other entity, including its affiliates and non-affiliates. (Opt-In)

III. Consumer Access

It is recommended that ~~A~~any consumer ~~should~~ have the ~~right~~ ability to submit a request to a licensee to obtain access to his/her personal information used by the licensee in its operations. Upon request, within a specified period of time, the licensee ~~should within 30 business days~~ provides a copy of the consumer's personal information, an explanation on how the personal information was used (*i.e.*, rating, underwriting, claims), and provides the source of the personal information. If personal information is in coded form, the licensee ~~should~~ would be expected to provide an accurate translation in plain language.

IV. Data Accuracy

It is recommended that ~~W~~within a specified period of time, ~~30 business days~~ after receiving a written request from a consumer to correct, amend, or delete personal information ~~used by the licensee in its operations,~~ within its possession the licensee ~~should~~ will either make the requested correction, amendment, or deletion or notify the consumer of its refusal to do so, the reasons for the refusal, and the consumer's right to file a statement of dispute setting forth what the consumer thinks is the correct information and the reasons for disagreeing with the licensee.

If the licensee corrects, amends, or deletes personal information, the licensee should notify any person or entity that has received the prior personal information within a specified period of time ~~the last 7 years~~. If the licensee does not correct, amend, or delete the disputed personal information, the licensee should notify any person or entity that has received the prior personal information within a specified period of time ~~the last 7 years of the consumer's statement of dispute~~.

V. Data Ownership and Portability

A consumer ~~customer~~ should have the right to request a copy of his/her personal information that he/she has provided to the licensee for use in the licensee's operations. A licensee should provide a consumer ~~customer~~ a copy of his/her personal information within a specified period of time ~~30 business days~~ of the request. Examples of this type of personal information include telematics data and "Internet of Things" ("IoT") data.

[Pull information from minutes pertaining to category of data ownership, post Summer Nat'l Mtg]

Office of Research Integrity {ORI} within the DHHS - Data Ownership. Data ownership refers to both the possession of and responsibility for information. The control of information includes not just the ability to access, create, modify, package, derive benefit from, sell or remove data, but also the right to assign these access privileges to others.

Scofield (1998) suggest replacing the term 'ownership' with 'stewardship', "because it implies a broader responsibility where the user must consider the consequences of making changes over 'his' data."

National Institute of Standards and Technology (NIST) – Information owner – An official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Data ownership formalizes the role of data owners and establishes accountability, assigning responsibility for managing data from creation to consumption. It puts rules and processes in place to ensure that the right people define usage directives, set quality standards, and consistently resolve data issues.

- Are there other points in the CO, VA, or Calif. laws that we want to include here?

MPL | MEDICAL PROFESSIONAL LIABILITY ASSOCIATION

ANALYSIS | INSIGHT | ADVOCACY

MPL Association Feedback
Privacy Protections Working Group's Privacy Policy Statement

Sec. I. Transparency –

In the insurer-policyholder context, this section would require an insurer to provide its privacy notice to a policyholder during the initial application process. It seems unnecessarily redundant to then require the insurer to provide its privacy notice to the policyholder when seeking additional information about the policyholder from third parties. Instead, the working group should clarify that the notice initially provided to a consumer must reference privacy policies and practices related to information which may later be obtained from a third party.

Sec. II. Consumer Control –

Section II requires licensees to allow consumers to opt-out of the sharing of their non-public personal information with third parties, except for specific purposes required or specifically permitted by law. While it is appropriate to leave the exception broad in this policy statement, we suggest including a reference that "specifically permitted by law" should always include the sharing of information with affiliated entities as necessary to conduct insurance operations, so as to deter the adoption of legislation which fails to include necessary exceptions such as those currently incorporated into Model #s 670 and 672.

Sec. IV. Data Accuracy –

It is not clear why Section IV adopts a 7-year threshold with respect to requiring a licensee to notify any person or entity that has received a consumer's personal information about the changes to that personal information. Stating that a threshold should be established, but allowing additional discussion to determine what that threshold should be, would be more appropriate.

Sec. III (Consumer Access) and Sec. V. (Data Ownership and Portability) –

The sections relating to Consumer Access (Section III) and Data Ownership and Portability (Section V) are virtually identical. Both give a consumer the right to request from a licensee a copy of their personal information used by the licensee in its operations. We would recommend merging these sections into one, unless there are distinctions between a consumer's access and data ownership/portability rights that the working group would like to address.

STATEMENT OF THE JOINT TRADES
CONCERNING THE
PRIVACY PROTECTIONS (D) WORKING GROUP'S
DRAFT "REPORT ON CONSUMER DATA PRIVACY PROTECTIONS"

December 2, 2021

The joint trades commend the Privacy Protections (D) Working Group (Working Group) for its commitment to the significant task of understanding the importance and background of the legal framework for consumer privacy protections. Protecting consumer privacy is a serious matter for consumers and insurers alike. In advance of the December 11 Working Group meeting, the joint trades[1] submit these comments concerning the November 18 exposure draft for your consideration.

The exposure document is composed of two parts, a draft Report and a draft Appendix. The draft Report is a thorough review of the existing legal landscape and summary of the Working Group conversations to-date. The draft Appendix is a privacy statement that has been described as a point for launching future discussion. To the extent the recommendations and Appendix are intended to serve as a foundation to expand on the legal and regulatory structure for insurance-related privacy requirements, such a foundation should be solid so that subsequent efforts to build on it are sound. Respectfully, the attached Exhibit A identifies inaccuracies and expresses concerns with the implications that regulators have determined that as a matter of public policy certain practices are expected without having been thoroughly discussed.

Referring back to the May 10th Working Group minutes, the NAIC Member-Adopted Strategy for Consumer Data Protections (Strategy) states that the deliverable for the Fall National Meeting is a report on the "charges" contained in the strategy. Based on that deliverable, the joint trades urge that the Working Group do one of three things:

> (1) (a) report to the Market and Regulation (D) Committee (D Committee) on the status of the Working Group's review of minimum appropriate consumer data privacy protections along with submission of a revised Report; and (b) recommend that a "Policy statement" is not necessary, instead, in the interest of time, the Privacy Working Group should begin a thorough, collaborative, and deliberate review of the Model laws and what, if any, revisions are necessary;
>
> (2) remove the Appendix and the Report's public policy recommendations and present that to the D Committee; or
>
> (3) delay the adoption of the exposure document, at least the Appendix, until stakeholders have sufficient time to comment on the document and the public policy positions stated in the Appendix can be fully discussed, debated, and voted on by Working Group Members.

While we appreciate the deliberate consideration of issues by the Working Group, we have significant concerns with the content and nature of the exposure of this particular document, the timelines for comment and adoption by the Working Group, and the form of Appendix A as a "NAIC Policy Statement."

[1] These comments are submitted jointly by the American Council of Life Insurers, the American Property Casualty Insurance Association, the Independent Insurance Agents & Brokers of America, and the National Association of Mutual Insurance Companies.

- The document was emailed to stakeholders on November 18 with the instruction that only "minor edits" would be accepted even though it is the first time that stakeholders were presented with the draft final work product of this Working Group and the document contains substantive new text in the form of an "NAIC Policy Statement," which calls for more than "minor edits."
- The document incorporates a "NAIC Policy Statement" that (i) had never been presented to stakeholders previously, and (ii) is misleadingly named because, to our knowledge, only reflects the views of the Working Group and not the NAIC membership writ large.
- Finally, these new documents were released on November 18, with a deadline of December 2 (with the meeting presenting them not held until November 22 and with Thanksgiving in the interim), giving stakeholders just two weeks to provide comments on new language that could have a significant impact. And, there will be no Working Group meeting between the December 2 comment deadline and the national meeting for comments to be discussed prior to the Working Group presumably adopting the document on December 11. The short comment period is presumably to allow time to incorporate any last minute edits into the document before the upcoming national meeting. We understand and appreciate the pressures that working groups and task forces may be under to complete their work in time for the last NAIC meeting of the year. Nonetheless, it is incumbent on a working group to provide a robust comment period, particularly with respect to a final work-product such as this.

We believe these procedural infirmities have led to substantive issues that go well-beyond the "minor edits" that were requested and have sought to provide questions and comments -- as best we are able on the timeframe -- in the attached exhibits.

To be certain, our expression of concern is not intended to delay the process but rather through the extensive feedback demonstrate our timely commitment to constructive and thorough engagement with regulators and consumer advocates. That said, please understand that the comments captured on the joint trade Exhibits reflect only what we have heard within the time provided and may not reflect all potential challenges posed by the exposure document.

We appreciate your consideration of these comments, and our organizations look forward to continued collaboration on this important issue. If you have any questions, please do not hesitate to reach out to any of our organizations.

EXHIBITS TO JOINT TRADE COMMENTS CONCERNING THE PRIVACY PROTECTIONS (D) WORKING GROUP'S DRAFT "REPORT ON CONSUMER DATA PRIVACY PROTECTIONS"

Given the shortness of time, these Exhibits contain examples to illustrate the themes expressed in the joint trades letter. It is not intended to be all-inclusive and the letter signatories therefore ask for the ability to supplement these comments and suggestions.

Appendix A

Appendix A - Overall: Comment

- Due to substantive concerns expressed below, the joint trades urge the Working Group to **delete Appendix A**.
- The "Policy Statement" is not necessary to meet the goals of the Working Group. It seems outside the NAIC norm for a Working Group to issue a policy statement of this type. As such, the Working Group might verbally report to the D Committee on the group's status of reviewing minimum appropriate consumer data privacy protections and recommend that as an **alternative** to this Appendix A, that the Working Group could begin moving forward with an analysis of whether to amend the model sections.

National Association of Insurance Commissioners

Privacy Protection (D) Working Group

Heading & Attribution: Comment

- If the Appendix is advanced, it **should specify** that it is a work product of the Privacy Protections (D) Working Group.
- The broader NAIC regulator membership hasn't had the opportunity to make an informed decision on the content of the items in the Appendix as a policy position of all insurance regulators.

Roadmap for Considering Additional Questions ~~Policy Statement~~ on Consumer Data Privacy Protections

Heading & Policy Statement: Comment

- If the Working Group maintains the Appendix, it should consider changing the title to a "Roadmap" to better identify its purpose.

Because the business operations of insurance companies are dependent upon the collection and use of personal information and data, state insurance regulators have long understood the need to balance an insurance company's need to collect consumer information and data with the consumer's right to limit the collection and use of data.

The NAIC adopted the *Insurance Information and Privacy Protection Model Act* (Model #670) in 1980 to establish standards for the collection, use and disclosure of information gathered in connection with insurance transactions. A key aspect of this model is that it establishes a regulatory framework for consumers to (1) ascertain what information is being or has been collected about them in connection with insurance transactions; (2) obtain access to such information for the purpose of verifying or disputing its accuracy; (3) limit the disclosure of information collected in connection with insurance transactions; and (4) obtain the reasons for any adverse underwriting decision. This regulatory framework is facilitated through a requirement that insurers or agents provide a written notice to all applicants and policyholders regarding the insurer's information practices.

Models: Comment

- The body of the Report contains information about existing Models. It appears **unnecessary** here.

The NAIC adopted the *Privacy of Consumer Financial and Health Information Model Regulation* (Model #672) in 2000. The model regulation was drafted to implement the requirements set forth in Title V of the federal *Gramm-Leach-Bliley Act* (P.L. 106-102) of 1999 (GLBA). GLBA imposed privacy and security standards on financial institutions and directed state insurance commissioners to adopt certain data privacy and data security regulations. The model also contains provisions governing protection of health information that were taken

directly from the Health Insurance Portability and Accountability Act Privacy Rule promulgated by HHS. The NAIC model regulation requires insurers to: (1) notify consumers about their privacy policies; (2) give consumers the opportunity to prohibit the sharing of their protected financial information with non-affiliated third parties; and (3) obtain affirmative consent from consumers before sharing protected health information with any other parties, affiliates, and non-affiliates. The key difference between the treatment of financial information and health information is that insurers must give consumers the right (with limited exceptions) to "opt out" of the disclosure or sharing of their financial information, but insurers must get explicit authorization ("opt in") before sharing health information.

Models: Comment

- The body of the Report contains information about existing Models. It appears **unnecessary** here.

This ~~policy statement~~ document is based on the consumer protections set forth in these two models and serves the purpose of informing forthcoming additional regulatory discussions and decisions regarding ~~licensed insurance entities, consumers, and the other state and federal regulatory agencies on what the NAIC currently supports as~~ the minimum consumer data privacy protections that are appropriate for inclusion in an NAIC model for the business of insurance. This ~~e policy statement~~ is not intended to modify any existing NAIC models and does not carry the weight of law or impose any legal obligations in states that have adopted those models.

NAIC Support for Minimum Consumer Data Privacy Protections: Comment

- Respectfully, the minimum consumer data privacy protections the NAIC supports ultimately will be presented in model amendments. These are incredibly important and detailed issues deserving careful thought. To have written documents indicating what the NAIC supports or stating what insurers "should" do might be taken out of context, potentially in litigation or elsewhere. Endorsing public policy outcomes of this nature is certainly premature, and it may leave companies vulnerable as well. These factors inform the joint trade request that the Working Group **remove** this Appendix or reframe it.

The Privacy Protections (D) Working Group Report on Consumer Data Privacy Protections ("Report") ~~policy statement~~ addresses consumer data privacy protections of (1) transparency; (2) consumer control; (3) consumer access; (4) data accuracy; and (5) ~~data ownership and~~ portability. ~~The policy statement~~ It intentionally excludes standards for cybersecurity and breach notification; data security and standards for the investigation and notification to an insurance commissioner of a licensed insurance entity's cybersecurity event~~, which~~ are the subject of separate model laws and interpretive guidance.

The following definitions are used for the purposes of this policy statement.

Definitions: Comment

- Including definitions in the Appendix for terms that are already defined in law or regulation may not be necessary in this document given that the models are described in the Report and are readily available. The joint trades recommend that all of the definitions be **removed** from this document.
- In some instances these definitions are modified versions of existing model law definitions. Unfortunately, the alterations expand the carefully drafted scope and requirements of the law. It is unclear whether this is intentional or whether it is inadvertent (in an effort to be brief). These deviations are not inconsequential - these details are meaningful.
- Our strong recommendation is to **eliminate** the definition section altogether. Definitions are foundational to setting legal expectations and requirements and, as such, they should mimic existing law unless and until there is agreement and discussion about any changes.

A. "Adverse Decision" means declination of insurance coverage, termination of insurance coverage, or charging a higher rate for insurance coverage on the basis of information which differs from that which the applicant or policyholder furnished~~, or denying a claim~~.

Definition of "Adverse Decision": Comment

- As an example of the impact in deviations, "adverse decision" is defined in the Appendix as "charging a higher rate for insurance coverage." However, Model 670 clarifies that this is "charging a higher rate on the basis of information which differs from that which the applicant or policyholder furnished." Additionally, a "denial of a claim" is not found in the existing Model 670 definitions.

B. "Consumer" means an individual who is seeking to obtain, obtaining, or have obtained a product or service to be used for personal, family, or household purposes from an insurer and about whom the insurer has nonpublic personal information. For example, an individual who has submitted an application for insurance is a consumer of the company to which he or she has applied, as is an individual whose policy with the company has expired.

Definition of "Consumer": Comment

- The document employs a definition of "Consumer" that deviates from the NAIC model definition without explanation, and this is an example of where it is unclear whether the Working Group was aiming to be brief or whether the group is contemplating revisions to what is in place in every state. Because this Appendix could be used to guide future action on privacy drafting work, common understanding and details matter. This further supports **removing** the definitions from this document altogether.

C. "Customer" means a consumer with whom an insurer has an on-going relationship.

D. "Licensee" means any insurer, producer, or other person licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to a state insurance law.

E. "Personal Information" means any individually identifiable information or data gathered in connection with an insurance transaction from which judgments can be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit, health, or any other personal characteristics. Personal information includes:

1. "Non-Public Personal Information," which means information that a consumer provides to a licensee to obtain an insurance product or service (like income, credit history, name and address); information about a consumer a licensee has as a result of a transaction involving an insurance product or service (like premium payment history, how much a life insurance policy is worth, and the value of personal property insured); and all other information about a consumer that a licensee uses in connection with providing a product or service to a consumer.

2. "Non-public personal health information," which means ~~any information that identifies a consumer in some way, and includes~~ information about a consumer's health, including past and present physical and mental health, details about health care, and payment for health care.

Definition of "Non-public Personal Health Information": Comment

- The definition of "nonpublic personal health information" reads as if the first clause could stand on its own and include any information that identifies a consumer in some way, which is not the case in existing law. We recommend **removing** the definitions (and the entire Appendix).

I. Transparency

Transparency: Comment

- The Transparency section illustrates the kinds of problems associated with framing these items as what "should" be done. Such framing implies that these things are either the case today or that regulators have thought through the implications of modifying the current requirements and have decided that such a change is necessary. These are two different things -- current requirements vs. potential future plans -- and they appear to be conflated here, not making it clear to the reader what is actually in law/regulation and what has been identified as worthy of revision.
- Turning to each of the paragraphs in this section clarifies the challenge and supports the ideas of **removing** this section and/or altering the nature of the document.

A licensee should provide a clear and conspicuous notice to consumers that accurately reflects its privacy policies and practices ~~when it first requests personal information about the consumer from the consumer or a third party~~.

Transparency & Notice Timing: Comment

- This paragraph, as drafted, simplifies the initial notice obligations and states that the licensee *should* provide notice when it first requests personal information.
- The timing representation isn't necessarily the requirement today, and there was no discussion about the possible challenges depending on what is meant by notice at "first request."
- Again, we believe that this has not been fully considered and could present challenges -- this supports the ideas of **removing** this section/paragraph and/or altering the nature of the document.

A licensee should also provide a revised ~~periodic~~ notice of its privacy policies and practices to customers ~~not less than annually~~ during the continuation of the customer relationship, if there is a substantive change in the licensee's privacy policy about which the customer has not been informed.

Transparency & Notice Timing: Comment

- The second paragraph states that a licensee *should* give a privacy notice at least annually during the continuation of the consumer relationship. This position is contrary to the decision made by the NAIC in 2017 to eliminate the redundant annual privacy notice requirements in a manner that was consistent with amendments to the Gramm-Leach-Bliley Act (GLBA) made in the Fixing America's Surface Transportation Act (FAST Act). To the best of our knowledge, all but nine states have implemented this annual notice modernization through statute, regulation, or bulletin.
- The specific wording edits shown above have not been fully vetted given the shortness of time. Again, this supports **removing** this section/paragraph.

If a licensee makes an adverse decision based on information/data that was not supplied by the consumers the licensee should provide the consumer with the specific reasons for the adverse decision upon request.

Transparency & Notice Timing: Comment

- The final paragraph within the Transparency Section relates to an adverse decision notice (and not to the privacy policy notice itself). If this is going to be included, it also calls for clarification consistent with existing law.
- Providing a consumer with the specific reasons for the adverse decision is to be done "upon request." This is something that should be recognized to reflect consistency with the existing balanced consumer privacy framework.
- Further, some are concerned that the wording is vague and are uncertain as to what it means, indicating that under some readings it could conflict with existing provisions in the insurance code, the FCRA, and other privacy laws.
- This paragraph would require careful thinking and reworking to make sense in the context of the concerns expressed. Given date, this supports **removing** this section/paragraph.

II. Consumer ~~Control~~ Preference Default Mechanism

Consumer Preference Heading: Comment

- From the section title of "consumer control" to the specifics of the statements made, there are several important concerns with this section that relate to the idea that such choices are not absolute.
- Rather than "control," wording like "preference" more appropriately sets expectations because there are numerous important exceptions -- and without these exceptions, operational and other aspects of the business of insurance could not function. If the concept is going to be included, the joint trades suggest **modifying** the heading.

Licensees should, at a minimum, provide consumers the opportunity to prohibit the sharing of their non-public personal information with third parties, except for specific purposes required or specifically permitted by law. (Opt-Out)

Licensees should obtain affirmative consent, except for specific purposes required or specifically permitted by law, from consumers before sharing non-public personal health information with any other entity, including its affiliates and non-affiliates. (Opt-In)

Consumer Control & Opt-In: Comment

- This is another area of the law that cannot necessarily be reduced to a simple statement about licensee obligations. There are legitimate and legally recognized reasons why a licensee should be able to share information without affirmative consent.
- Indeed, regulator statements were made during a public Working Group meeting that indicated an understanding of the fact that certain exceptions are essential.
- If the document is going to remain in this form, the Opt-In section must be **amended** to recognize this: "Licensees should obtain affirmative consent, *except for specific purposes required or specifically permitted by law*, from consumers before sharing non-public personal health information with any other entity, including its affiliates and non-affiliates."

III. Consumer Access

Any consumer should have the right to submit a request to a licensee to obtain access to his/her personal information used by the licensee in its operations. Upon request, subject to certain exceptions and verification procedures, the licensee should ~~within 30 business days~~ provide a copy of the consumer's personal information in the timeframe established by law~~, an explanation on how the personal information was used (i.e., rating, underwriting, claims), and provide the source of the personal information~~. ~~If personal information is in coded form, the licensee should provide an accurate translation in plain language.~~

Consumer Access: Comment

- Consumer access should be qualified to reflect considerations like anti-fraud, identity theft, and security. Verification of the consumer and the request are critical components.
- Also, exceptions to provision of certain information should be recognized. It would be exceptionally burdensome to enumerate "the source of the personal information." This is not required by other laws. For example, CPRA requires disclosure of the categories of sources from which the consumer's personal information was collected. That approach potentially strikes a more appropriate balance to ensure meaningful disclosure without adding significant cost to industry that will have little consumer benefit. Perhaps the intent here was to mirror the California approach, but this is not what the words here indicate.
- Another way that this paragraph adds confusion is by reference to "how the personal information was used," which goes beyond even CCPA.
- The 30 day requirement is more nuanced in law and only requires provisions of the "nature and substance" of personal information and a generalized summary of where it's from and how it is disclosed. To expect anything more as suggested by this paragraph, 30 days would be an extremely difficult obligation to meet. For instance, CCPA gives companies 45 days and that 45 days can be extended an additional 45 days if necessary.
- There is also uncertainty as to what it means to provide personal information that is in a coded form in an accurate plain language translation. Is this a summary of data or a copy of the data? This appears to be a new requirement that deserves consideration.
- Finally, unstructured or non-searchable data should not be contemplated. As you can see, there are many important aspects to this discussion. We urge you not to include this and other "should" provisions that have not prompted discussion and debate around the practical details. There are so many concerns with this provision, we urge you to **delete** it.

IV. Data Accuracy

Within 30 business days after receiving a written request from a consumer to correct, amend, or delete personal information within its possession ~~used by the licensee in its operations~~, the licensee should either make the requested correction, amendment, or deletion or notify the consumer of its refusal to do so, the reasons for the refusal, and the consumer's right to file a statement of dispute setting forth what the consumer thinks is the correct information and the reasons for disagreeing with the licensee.

Data Accuracy & Request (30 Days): Comment

- Several practical aspects from Section 9 of Model #670 are missing. These details matter. If this is included here, we recommend reviewing these details and making **edits** accordingly.

If the licensee corrects, amends, or deletes personal information, the licensee should notify any person or entity that has received the prior personal information in the manner and within the timeframe established by law. ~~within the last 7 years. If the licensee does not correct, amend, or delete the disputed personal information, the~~

~~licensee should notify any person or entity that has received the prior personal information within the last 7 years of the consumer's statement of dispute~~.

Data Accuracy & Notify Others (7 Years): Comment

- There was no public discussion of the broad new 7 year look back period referenced here. This seems very broad and onerous and potentially inconsistent with record retention policies, and it may have the unintended consequence of increasing privacy concerns. For example, if a vendor relationship was entered into six years ago, but ended four years ago and data has been archived or deleted, the obligation to notify would still apply. What about instances where business information is shared for a one-time use? Or limited by a business relationship?
- Notifying all recipients within the last seven years will present a significant burden to industry with little consumer benefit and absurd results. Because the statement is inconsistent with existing law, such substantive changes should be the subject of future detailed discussion. As such, we urge you to **delete** it altogether.

V. Data ~~Ownership and~~ Portability

Data portability is a complex issue that must be thoroughly discussed so that if any additional regulatory pronouncements are warranted they are clearly delineated to provide licensees with achievable compliance obligations. ~~A customer should have the right to request a copy of his/her personal information that he/she has provided to the licensee for use in the licensee's operations. A licensee should provide a customer a copy of his/her personal information within 30 business days of the request. Examples of this type of personal information include telematics data and "Internet of Things" ("IoT") data.~~

Data Ownership and Portability: Comment

- This topic has not yet been discussed in any detailed or meaningful way by the Working Group. Additional discussion may be warranted, but it is premature for the group to reach conclusions at this point about whether or how this complicated subject matter should be addressed.
- On the subject of timing, requests for a copy of a customer's data is not a simple request. Thirty days could be very difficult to meet.
- These are not concepts in the existing NAIC model laws.
- Experience with the GDPR has proven portability can be problematic raising many practical questions on what data and in what format based on different processing systems.
- The specific mention of telematics and internet of things data in the ownership and portability section could warrant another stand-alone project as it raises many questions. For example, what does telematics and internet of things data mean? Further, it is unclear to what degree such information is even able to be provided in a portable format and there may be trade secret or other confidential information included with that type of data, depending on how broadly it is construed. This sentence should be **stricken**.

EXHIBITS TO JOINT TRADE COMMENTS CONCERNING THE PRIVACY PROTECTIONS (D) WORKING GROUP'S DRAFT "REPORT ON CONSUMER DATA PRIVACY PROTECTIONS"

A: APPENDIX
Comments Highlighting Concerns

➤ B: REPORT
Suggested Revisions

Given the shortness of time, these Exhibits contain examples to illustrate the themes expressed in the joint trades letter. It is not intended to be all-inclusive and the letter signatories therefore ask for the ability to supplement these comments and suggestions.

Privacy Protections (D) Working Group Report on

Consumer Data Privacy Protections

Exposure Draft

November 18, 2021

[...]

I. Introduction

The Privacy Protections (D) Working Group was appointed in 2019 to review state insurance privacy protections regarding the collection, use, and disclosure of information gathered in connection with insurance transactions and make recommended changes, as needed, to NAIC models addressing privacy protection. This includes an insurer's use of data collected from a consumer and data supplied to an insurer by a third-party vendor. ~~Rather than focusing on revisions to NAIC models, the main deliverables for 2021 were to set forth a policy statement on the minimum consumer privacy protections that are appropriate for the business of insurance, after taking into consideration the consumer privacy protections that already exist under applicable state and federal laws.~~

Introduction & 2021: Comments

Based on broader joint trade recommendations relating to the Appendix, we suggest that the last sentence be **deleted**. In addition to the general concerns regarding the "policy statement" it seems that this framing of the purpose of the Report appears to be inconsistent with the way it is described within the exposure draft (on page 13).

The Working Group discussed how best to balance the need for information by those conducting the business of insurance and the public's need for fairness in insurance information practice ~~rights of insurers to use data for legitimate business purposes with consumers' rights to control what data is used and how it is used~~. The following privacy protections for consumers were discussed: (1) the right to opt out of data sharing, (2) the right to limit data sharing unless the consumer opts in, (3) the right to correct information, (4) the right to delete information, (5) the right of data portability, (6) the right to restrict the use of data, (7) the right of data ownership, (8) the right of notice, and (9) the right of nondiscrimination / non-retaliation.

Introduction & Balance: Comments

To be consistent with Model #670 and to be clearer with respect to the scope of the balance, we recommend this **revision**.

The Working Group received comments from the ACLI, AHIP, APCIA, BCBSA, the Coalition of Health Insurers, NAMIC, MLPA, and NAIC consumer representatives Birny Birnbaum, Brenda Cude, Karrol Kitt, and Harry Ting.

[...]

V. Summary of General Data Protection Regulation (GDPR)

The GDPR became effective in May 2018 and may apply ~~applies~~ to U.S. companies based on whether or not they process the ~~if they collect~~ data from citizens of the E.U. or are processing data within the E.U and provided that they have a sufficient nexus with the E.U~~over the internet~~. It requires companies (data "controllers") to obtain explicit consent from consumers to collect their data ("opt in") with an explanation of how the data will be used. It also contains standards for safeguarding the data collected. Under the GDPR, a consumer has the following rights: (1) to receive information about the processing of personal data; (2) to obtain access to the personal data; (3) to request that incorrect, inaccurate or incomplete personal data be corrected; (4) to request that personal data be erased when it is no longer needed or if processing it is unlawful; (5) to object to the processing of personal data for marketing purposes or on grounds relating to a consumer's particular situation; (6) to request the restriction of the processing of personal data in specific cases; (7) to receive personal data in a machine-

readable format and the ability to send it to another controller ("data portability"); and (8) to request that decisions based on automated processing concerning the consumer or significantly affecting the consumer and based on consumer's personal data, are made by human beings.

GDPR Summary: Comments

CLARIFICATION: The GDPR does not, necessarily, apply to a company simply because it collects data from citizens of the EU over the internet. More is required. Specifically, the company must actively market its products and services to those in the EU. It is a factual determination. For example, routinely shipping goods to the EU, utilizing the French language on the website (in addition to English) and setting the website up to accept euros would likely result in the GDPR applying to a given company.

VI. Summary of Recently Adopted Consumer Privacy Protection Laws

A. California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)

[...]

Consumer Rights

California law provides consumers with the following rights, subject to certain limitations: (1) to request deletion of any personal information;[1] (2) to correct inaccurate personal information, taking into account the nature of the personal information and the purposes of the processing of the information; (3) to know about and access the personal information being collected by requesting that the business disclose: the categories and specific pieces of personal information collected, the categories of sources the information was collected from, the business purpose for collecting the information, the categories of third parties with whom the information is shared, and the specific pieces of personal information that was shared; (4) to request the personal information provided by the consumer in a format that is easily understandable, and to the extent technically feasible, in a structured, commonly used, machine-readable format that may also be transmitted to another entity at the consumer's request without hindrance; (5) to know what personal information is sold or shared and to whom; (6) to opt out of the sale or sharing of personal information; (7) to limit the use and disclosure of sensitive personal information; and (7) to not be retaliated against for requesting to opt out or exercise other rights under the law.

Summaries of Consumer Rights: Comments

The consumer rights under the referenced laws are not absolute. In terms of describing the various rights contained within the state privacy laws noted (CA, CO, and VA), such descriptions should be prefaced with "subject to certain limitations." It is important that there is an understanding of this by all readers of the Report. A similar clarification should be made in the corresponding descriptions of the other jurisdictions as well.

[...]

VII. Summary of Working Group Discussions of Selected Key Points

The Working Group began discussions Dec. 8, 2019, during the Fall National Meeting with the following minimum consumer privacy protections being considered as appropriate for the business of insurance. These rights were based on the Working Group's proposed 2020 charges and are included in the Working Group's initial 2019 Work Plan:

1. the right to receive notice of an insurer's privacy policies and practices;

2. the right to limit an insurer's disclosure of personal data;

3. the right to have access to personal data used by an insurer;

4. the right to request the correction or amendment of personal data used by an insurer;

5. the right of data ownership; and

6. the right of data portability.

Rights: Comments

To avoid confusion for readers of the Report, the joint trades highly recommend that the Working Group **insert a footnote** to the exposure document to clarify that these are more precisely "issues" or "rights to request," given important legal/regulatory reporting requirements and other operational exceptions. This is crucial to continuing to advance constructive discussion on these issues.

[...]

Working Group discussions revealed that state insurance regulators and consumer representatives believe consumers own the data that is collected and used by the insurance industry to market, sell, and issue insurance policies. It was felt that the type of data collected (name, age, date of birth, height, weight, income, physical condition, personal habits, etc.) describes who a person is and distinguishes one person from another by its very nature. When a consumer shares their data with an insurance company, it is with the understanding that the consumer is letting the company borrow it for a time to determine what insurance rates and insurance coverage the consumer needs. The consumer is not giving up their data to an insurer so it can be sold or given to other organizations from whom the consumer is not seeking insurance coverage, or any other product. ~~Consumer representatives indicated~~ they believe ~~that this practice had happened when they did an online search for insurance rates on health plans. As a result, the consumer representative~~ reports ~~to subsequently having received hundreds of cold calls from companies selling products other than insurance. When the consumer representative asked with whom the insurance company shared his data, the company sent him a list of 1,700 companies – none of which sold insurance.~~

Belief Online Insurance Search Yielded Hundreds of Cold Calls: Comments

The last three sentences appear to be anecdotal in nature. We suggest that the sentences be **removed**. If they are retained, please edit them to reflect that the words be revised to reflect that this is what was believed and reported.

~~The privacy policy statement in Appendix A is designed to be the foundation for the minimum consumer data privacy protections that are appropriate for the business of insurance to be applied to NAIC model #672 as revisions. It~~ This Report is intended to kick-start the next step in creating revisions by defining the parameters of the existing consumer data privacy rights~~; by suggesting definitions and by showing examples of consumer risks~~. Further discussion is necessary, however, to clarify consumer data privacy rights that may not be fully protected in federal laws or fully covered under NAIC Model laws, and to decide how to provide appropriate protections.

"Policy Statement" & Appendix A: Comments

Based on substantive concerns expressed in other exhibits and on the alternatives offered, the joint trades strongly urge that this paragraph be **edited** to provide ample flexibility for the forthcoming Working Group efforts while still satisfying 2021 objectives. Indeed, as you will see from Exhibit A, the most serious concerns of the joint trades are in that document. **Because it is not necessary to meet the aims of the Working Group, we urge removing the Appendix.**

VIII. Conclusion and Recommendations

Months of detailed discussions with regulator, industry, and consumer stakeholders, and the comments they have submitted, have led the Working Group to determine that the *NAIC Insurance Information and Privacy Protection Model Act (Model #670)* and the *Privacy of Consumer Financial and Health Information Regulation (Model #672)* have in the past provided an effective regulatory framework for consumer privacy protections to oversee and enforce consumer data privacy as required by state and federal statutes and regulation. ~~However, t~~These models were adopted by the NAIC 20 and 40 years ago, respectively; with only 17 jurisdictions adopting Model #670.

Existing Models: Comment

The existing NAIC Models focus on concepts and are largely not technology-specific. Because the regulators had the foresight to be more principles-oriented than prescriptive, much of what those models offer remain valuable to states today. With this in mind, the joint trades suggest this **minor edit**.

In consideration of the many changes that have occurred in recent years, as well as the rate of increase in the use of new technologies (AI, machine learning, accelerated underwriting, rating algorithms, etc.), and big data by insurers, the Working Group recommends additional consideration of the ways that models 670 and/or 672 could be amended to ensure that regulators and legislators can continue to have a robust menu of options to provide consumer data privacy protections essential to meet the consumer data privacy challenges presented by the public use of technology and data by insurers in today's business environment.

Existing Models: Comment

Building on the paragraph above, it seems worthwhile for regulators to consider whether and how the new technology may impact the business of insurance, including privacy practices. With this in mind, the joint trades suggest these **clarifying edits**.

Subsequent to systematic and transparent decisions relating to Appendix A and adoption of any model changes, the Working Group also recommends the NAIC's Market Regulation Handbook be updated, as necessary, to provide guidance to state insurance regulators so they can verify insurers' compliance with the state's regulatory framework for consumer privacy protections.

Handbook: Comment

To be clear about the process, it seems that the Handbook cannot be updated until after the models have been adopted. With this in mind, the joint trades suggest this **edit**.

Arbor Strategies, LLC

Chris Petersen
804-916-1728
cpetersen@arborstrategies.com

December 2, 2021

Ms. Cynthia Amann
Chair, NAIC Privacy Protections (D) Working Group
Missouri Department of Insurance
301 W High St Rm 530
Jefferson City, MO 65101

Dear Ms. Amann:

I am writing on behalf of a Coalition of health insurers, who represent some of the country's largest major medical insurers and health maintenance organizations, to comment on the NAIC Privacy Protections (D) Working Group's ("Working Group") proposed Privacy Protections (D) Working Group Report on Consumer Data Privacy Protections Exposure Draft dated November 18, 2021 ("Exposure Draft"). As I noted on the Working Group's last conference call, the Coalition has concerns with the Exposure Draft ranging from technical issues with how policy decisions in existing NAIC models are portrayed to process issues to questions regarding the necessity of drafting a new privacy model. As a result of these concerns, the Coalition cannot support the Exposure Draft as written. The Working Group should defer action on the Exposure Draft in order to address the many concerns that we, and others in the industry, have raised regarding the Exposure Draft.

Our technical concerns are centered in Appendix A of the Exposure Draft which the Working Group indicated is intended to reflect areas of agreement or, at a minimum, areas that should be addressed more fully. The Exposure Draft suggests that the statements in Appendix A reflect positions previously taken by the NAIC in either Model 670 or Model 672. However, several of these statements are inaccurate and do not reflect current NAIC privacy policy. I attached a redlined version of Appendix A that highlights all of our concerns, but I would like to highlight three issues in particular.

First, under heading I. Transparency Appendix A states that a "licensee should also provide a periodic notice of its privacy policies and practices to customers not less than annually during the continuation of the customer relationship." Neither Model 670 nor Model 672 require annual notices. In fact, during one of its recent revisions to Model 672 the NAIC

eliminated the requirement for annual notices, determining that in "most cases an annual notice is not necessary."

Second, in II. Consumer Control it provides "Licensees should obtain affirmative consent from consumers before sharing non-public personal health information with any other entity, including its affiliates and non-affiliates." The Working Group, in multiple discussions agreed that health plans can, and in some cases must, make disclosures that are required or permitted by law. However, this caveat is not reflected in the Appendix A policy statement. It is not accurate to simply aver that "licensees should obtain affirmative consent," without also making clear that this position must be nuanced to prevent significant consumer harm if personal health information is withheld inappropriately. The "required or otherwise permitted" language appears, although without full discussion, in the section relating to opt out, but it does not appear in the opt in discussion.

Finally, Appendix A does not include any discussion of the HIPAA safe harbor policy that is included in Model 672. This issue was discussed several times in the public meetings of the Working Group, generally with favorable comments from Working Group members. The Coalition, at least, came away with the impression that the Working Group supported the concept. Despite this apparent support, the HIPAA safe harbor is not discussed in the policy paper. This omission has the potential to cause serious harm to the health insurance market, consumers and the smooth functioning of the health care system. The Coalition cannot support any document that does not include the HIPAA safe harbor.

The Coalition also has concerns with the process under which the Exposure Draft was developed. It appears that there were up to eleven closed meetings where interested parties were not allowed to participate. What is particularly troubling about these meetings is that it appears that significant policy decisions, including, at a minimum, the annual notice requirement, the lack of a HIPAA safe harbor, and a requirement that insurers get authorization before disclosing health information, even if the disclosure was required by law, were made during these closed meetings. Although the purpose of the meetings was to allow regulatory subject matter experts to discuss issues, we believe these discussions would have been more fruitful if interested party subject matter experts also participated.

The Exposure Draft also states that "the Working Group recommends that models 670 and 672 be amended to ensure that regulators can continue to provide consumer data privacy protections essential to meet the consumer data privacy challenges presented by the public use of technology and data by insurers in today's business environment." Much of the discussion

needed to reach this decision must have occurred in closed session. This is a fairly significant decision to make without the full input from all interested parties and is a decision that the Coalition does not support. We also question whether a model that has only been adopted by 16 states (Model 670) can be amended under the NAIC's new rules which require that two thirds of the voting members must agree to enact the model before voting to adopt the model in their home states.

This segues into the Coalition's final concern regarding the need to draft a new model or to revise the existing NAIC models. As noted above, the Coalition does not believe it would be appropriate to revise Model 670. It has not generated significant state interest or activity to warrant amending. Under today's NAIC rules the model would not even be eligible to been adopted unless a majority of states agree to make best efforts to have it adopted by their state legislatures. If it cannot be adopted, it should not be amended. It is also not necessary to amend Model 670 if all of the concepts from the Exposure Draft are amended into Model 672.

It would also be much easier to amend Model 672. Model 672 reflects present NAIC thinking on how to address these issues and it includes the most up to date language and vernacular when addressing privacy issues. It also would not require the removal of several out-to-date provisions as would be required if the Working Group chose to amend model 670. With that said, it might not even be necessary to revised either of the models. The Working Group should develop a white paper identifying key issues and then pointing them to specific model language that addresses the issue. Rather than adopting revisions to Model 670 and Model 672, the Working Group should prepare a road map to help states address privacy issues that a state might want to consider.

Thank you for the opportunity to comment. If you have any questions, please feel free to reach out to me at either (202) 247-0316 or cpetersen@arborstrategies.com. We look forward to working with the Working Group as it reviews these comments and other comments submitted by interested parties.

Sincerely yours,

Chris Petersen
Arbor Strategies, LLC

cc: Lois Alexander

Appendix A

National Association of Insurance Commissioners
Policy Statement on Consumer Data Privacy Protections

Because the business operations of insurance companies are dependent upon the collection and use of personal information and data, state insurance regulators have long understood the need to balance an insurance company's need to collect consumer information and data with the consumer's right to limit the collection and use of data.

The NAIC adopted the *Insurance Information and Privacy Protection Model Act* (Model #670) in 1980 to establish standards for the collection, use and disclosure of information gathered in connection with insurance transactions. A key aspect of this model is that it establishes a regulatory framework for consumers to (1) ascertain what information is being or has been collected about them in connection with insurance transactions; (2) obtain access to such information for the purpose of verifying or disputing its accuracy; (3) limit the disclosure of information collected in connection with insurance transactions; and (4) obtain the reasons for any adverse underwriting decision. This regulatory framework is facilitated through a requirement that insurers or agents provide a written notice to all applicants and policyholders regarding the insurer's information practices.

The NAIC adopted the *Privacy of Consumer Financial and Health Information Model Regulation* (Model #672) in 2000. The model regulation was drafted to implement the requirements set forth in Title V of the federal *Gramm-Leach-Bliley Act* (P.L. 106-102) of 1999 (GLBA). GLBA imposed privacy and security standards on financial institutions and directed state insurance commissioners to adopt certain data privacy and data security regulations. The model also contains provisions governing protection of health information that were taken directly from the Health Insurance Portability and Accountability Act Privacy Rule promulgated by HHS. The NAIC model regulation requires insurers to: (1) notify consumers about their privacy policies; (2) give consumers the opportunity to prohibit the sharing of their protected financial information with non-affiliated third parties; and (3) obtain affirmative consent from consumers before sharing protected health information with any other parties, affiliates, and non-affiliates. The key difference between the treatment of financial information and health information is that insurers must give consumers the right (with limited exceptions) to "opt out" of the disclosure or sharing of their financial information, but insurers must get explicit authorization ("opt in") before sharing health information.

This policy statement is based on the consumer protections set forth in these two models and serves the purpose of informing licensed insurance entities, consumers, and the other state and federal regulatory agencies on what the NAIC currently supports as the minimum consumer data privacy protections that are appropriate for the business of insurance. The policy statement is not intended to modify any existing NAIC models and does not carry the weight of law or impose any legal obligations in states that have adopted those models.

The policy statement addresses consumer data privacy protections of (1) transparency; (2) consumer control; (3) consumer access; (4) data accuracy; and (5) data ownership and portability. The policy statement intentionally excludes standards for data security and standards for the investigation and notification to an insurance commissioner of a licensed insurance entity's cybersecurity event, which are the subject of separate model laws and interpretive guidance.

The following definitions are used for the purposes of this policy statement.

A. "Adverse Decision" means declination of insurance coverage, termination of insurance coverage, charging a higher rate for insurance coverage, or denying a claim.
B. "Consumer" means an individual who is seeking to obtain, obtaining, or have obtained a product or service from

an insurer. For example, an individual who has submitted an application for insurance is a consumer of the company to which he or she has applied, as is an individual whose policy with the company has expired.

C. "Customer" means a consumer with whom an insurer has an on-going relationship.

D. "Licensee" means any insurer, producer, or other person licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to a state insurance law.

E. "Personal Information" means any individually identifiable information or data gathered in connection with an insurance transaction from which judgments can be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit, health, or any other personal characteristics. Personal information includes:

1. "Non-Public Personal Information," which means information that a consumer provides to a licensee to obtain an insurance product or service (like income, credit history, name and address); information about a consumer a licensee has as a result of a transaction involving an insurance product or service (like premium payment history, how much a life insurance policy is worth, and the value of personal property insured); and all other information about a consumer that a licensee uses in connection with providing a product or service to a consumer.
2. "Non-public personal health information," which means any information that identifies a consumer in some way, and includes information about a consumer's health, including past and present physical and mental health, details about health care, and payment for health care.

I. Transparency

A licensee should provide a clear and conspicuous notice to consumers that accurately reflects its privacy policies and practices when it first requests personal information about the consumer from the consumer or a third party.

A licensee should also provide a periodic notice of its privacy policies and practices to customers not less than annually during the continuation of the customer relationship.
Model 672 §6.A., but *see* Model 672 §6.B. which provides in most cases an annual notice is not necessary
Model 670 does not require an annual notice

If a licensee makes an adverse decision based on information/data that was not supplied by the consumer, the licensee should provide the consumer with the specific reasons for the adverse decision.

II. Consumer Control

Licensees should, at a minimum, provide consumers the opportunity to prohibit the sharing of their non-public personal information with third parties, except for specific purposes required or specifically permitted by law. (Opt-Out)
See Model 672 §12.A. and see Model 672 §§16-18. Note, however, that Section 12 only applies to opting out of disclosures to nonaffiliated third parties. The statement above would appear to go further than Model 672 and applying the opt out requirements to all third parties.

Licensees should obtain affirmative consent from consumers before sharing non-public personal health information with any other entity, including its affiliates and non-affiliates. (Opt-In)
Model 670 §13.A. and Model 672 §18.A. However, the above statement omits the key phrase that an authorization is not needed if the disclosure is required by law or otherwise permitted by law. *See* Model 672 §18.B. and Model 670 §13. B.-R.

III. Consumer Access

Any consumer should have the right to submit a request to a licensee to obtain access to his/her personal information used by the licensee in its operations. Model 670 §8.A Upon request, the licensee should within 30 business days provide a copy of the consumer's personal information Model 670 provides alternatives to providing copies such as oral communications an explanation on how the personal information was used (i.e., rating, underwriting, claims), this right is not included in Model 670 and provide the source of the personal information. Model 670 only requires insurance institutions to identify the source of the information if such source is an institutional source. Model 670 §8.B. If personal information is in coded form, the licensee should provide an accurate translation in plain language.

IV. Data Accuracy

Within 30 business days after receiving a request from a consumer to correct, amend, or delete personal information used by the licensee in its operations, the licensee should either make the requested correction, amendment, or deletion or notify the consumer of its refusal to do so, the reasons for the refusal, and the consumer's right to file a statement of dispute setting forth what the consumer thinks is the correct information and the reasons for disagreeing with the licensee.

If the licensee corrects, amends, or deletes personal information, the licensee should notify any person or entity that has received the prior personal information within the last 7 years. This incorrectly states the provisions of Model 670. The Model provides that insurance institutions must only notify those persons *specifically designated by the individual* who may have, … received such recorded personal information…*See* Model 670 §9.B.1. Model 670 also only has a "look back" requirement of 2 years not the 7 years included in the statement above. *See also* Model 670 §9.B.1. If the licensee does not correct, amend, or delete the disputed personal information, the licensee should notify any person or entity that has received the prior personal information within the last 7 years of the consumer's statement of dispute. *See* comment above.

V. Data Ownership and Portability

A customer should have the right to request a copy of his/her personal information that he/she has provided to the licensee for use in the licensee's operations. A licensee should provide a customer a copy of his/her personal information within 30 business days of the request. Examples of this type of personal information include telematics data and "Internet of Things" ("IoT") data.

See Model 670 §8.A regarding access to information, but query as to whether the information cited in this paragraph is included with the definition of "personal information" found in Model 670 at §2.T. If this information is not personal information and the Working Group is considering expanding the models to nonpersonal information that would be a significant departure from existing privacy law.

BlueCross BlueShield Association

An Association of Independent Blue Cross and Blue Shield Plans

December 2, 2021

Ms. Cynthia Amann, Chair
Mr. Ron Kreiter, Vice Chair
Privacy Protections (D) Working Group
National Association of Insurance Commissioners

Submitted electronically to: Lois Alexander (lalexander@naic.org)

RE: Comments on the draft Report to the Market Regulation and Consumer Affairs (D) Committee on Consumer Data Privacy Protections (Final Exposure Draft 11.18.21)

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

The Blue Cross Blue Shield Association (BCBSA) appreciates the opportunity to provide comments on the draft Report on Consumer Data Privacy Protections, exposed on November 18, 2021.

BCBSA is a national federation of 35 independent, community-based and locally operated Blue Cross and Blue Shield (BCBS) companies (Plans) that collectively provide health care coverage for one in three Americans. For more than 90 years, Blue Cross and Blue Shield companies have offered quality health care coverage in all markets across America — serving those who purchase coverage on their own, as well as those who obtain coverage through an employer, Medicare and Medicaid.

BCBSA commends the Privacy Protections (D) Working Group (PPWG or working group) for its commitment to protecting consumer privacy and for its work to identify appropriate protections for the business of insurance. However, for the reasons below, we do not agree that the policy statement, in its current form, should be advanced. BCBSA recommends that the policy statement should focus on articulating the current state of laws and models on government privacy protections and outline issues open for consideration.

We would like to express support for several of the comments made during the November 22, 2021 working group call. BCBSA shares the concerns of other commenters regarding the current uncertainty of whether a HIPAA exemption will be included in this document, how certain terms are defined, and the process by which the working group drafted the report and recommendations.

Based on discussions during the November 22 call, it is our understanding that the working group has not yet decided whether to include a HIPAA exemption. BCBSA strongly urges the working group to articulate support for the inclusion of a HIPAA exemption. As we have stated in previous comments, the existing HIPAA Privacy Rule regime and state laws should not be displaced by new requirements, and an exemption should be maintained for health insurers that are compliant with HIPAA and applicable state laws.

We believe the working group should clarify its definitions of terms such as opt-in, opt-out, and

portability, to describe more accurately what the terms mean. As currently written, they are defined differently than commonly used. In some cases, the definition is inconsistent with its definition in NAIC Model #672, such as with “opt-out”. BCBSA agrees that clarification and consistency is needed.

Accompanying our letter is a redline that captures our suggested revisions to the report. BCBSA also offers the proposed substantive revisions:

- **Summary of Health Insurance Portability and Accountability Act (HIPAA):** BCBSA believes this section could benefit from more specificity to achieve a more accurate description of the law; we have provided suggested language for consideration.

- **Summary of Recently Adopted Consumer Privacy Protection Laws:** BCBSA believes the Working Group should explicitly state in the report that the California Consumer Privacy Act includes a HIPAA exemption.

- **Conclusion and Recommendations:** The working group recommends revisions to Models #670 and #672 due to the many changes that have occurred in recent years, particularly regarding new technologies. In anticipation of future changes, BCBSA encourages the working group to focus its revisions on Model #672. Model #672 is more reflective of the current regulatory thinking and attitudes on privacy protections. Further, the working group indicated in a previous meeting that Model #672 would be the foundation for its work. Also, Model #670 has not been accepted as broadly throughout the states as Model #672. BCBSA also encourages the PPWG to clarify the process for how model laws will be further amended in the context of federal privacy laws and when new data elements are added.

- **Appendix:** Under Consumer Control, BCBSA recommends adding references to HIPAA at the end of the first sentence. We also recommend deleting the second sentence referred to as “opt-in” as it is inconsistent with HIPAA.

  In the Data Accuracy section, we recommend a sentence clarifying that the provisions in this section align with HIPAA requirements and HIPAA covered entities should be exempted from additional requirements as specified.

  We also recommend deleting the last sentence in Data Ownership and Portability because we believe the examples provided by the working group are too broad.

BCBSA would like to thank the working group for its consideration of our comments. If you have questions, please contact Randi Chapman, managing director, state relations, at Randi.Chapman@bcbsa.com or Lauren Choi, managing director for health data and technology policy, at Lauren.Choi@bcbsa.com.

Sincerely,

Clay S. McClure
Executive Director, State Relations

Privacy Protections (D) Working Group Report on Consumer Data Privacy Protections

Exposure Draft

November 18, 2021

Table of Contents

I. Introduction

The Privacy Protections (D) Working Group was appointed in 2019 to review state insurance privacy protections regarding the collection, use, and disclosure of information gathered in connection with insurance transactions and make recommended changes, as needed, to NAIC models addressing privacy protection. This includes an insurer's use of data collected from a consumer and data supplied to an insurer by a third-party vendor. Rather than focusing on revisions to NAIC models, the main deliverables for 2021 were to set forth a policy statement on the minimum consumer privacy protections that are appropriate for the business of insurance, after taking into consideration the consumer privacy protections that already exist under applicable state and federal laws.

The Working Group discussed how best to balance the rights of insurers to use data for legitimate business purposes with consumers' rights to control what data is used and how it is used. The following privacy protections for consumers were discussed: (1) the right to opt out of data sharing, (2) the right to limit data sharing unless the consumer opts in, (3) the right to correct information, (4) the right to delete information, (5) the right of data portability, (6) the right to restrict the use of data, (7) the right of data ownership, (8) the right of notice, and (9) the right of nondiscrimination / non-retaliation.

The Working Group received comments from the ACLI, AHIP, APCIA, BCBSA, the Coalition of Health Insurers, NAMIC, MLPA, and NAIC consumer representatives Birny Birnbaum, Brenda Cude, Karrol Kitt, and Harry Ting.

II. Overview of Issue

Consumer awareness and regulatory concerns about the use of consumer data by a variety of commercial, financial, and technology companies are increasing. This has led to adoption of the General Data Protection Regulation (GDPR) in the E.U. and the California Consumer Privacy Act (CCPA) and other state data privacy protection laws in the U.S. Though data privacy concerns extend beyond the insurance sector, the increasing use of data and the passage of these new laws is causing the insurance industry and consumer groups alike to pressure Congress to enact federal privacy legislation.

While federal legislative efforts are currently stalled due to other legislative priorities and differing perspectives from consumers and industry on the best path forward, it is likely that Congress will begin focusing on the issue again soon. The current pause provides state insurance regulators an opportunity to update state privacy protections consistent with the current insurance business environment and potentially forestall or mitigate the impacts of any preemptive federal legislation. State policymakers have also responded to the privacy debate with varying legislative proposals to provide consumers with greater transparency and control over the use of personal information, with California, Virginia, and Colorado being leading examples. These comprehensive state data privacy laws each have either entity-level or data-level exemptions for entities subject to or information collected pursuant to the federal Gramm-Leach-Bliley Act (GLBA) and/or the privacy regulations adopted under the Health Insurance Portability and Accountability Act (HIPAA).

III. Summary of Consumer Privacy Protections Provided by NAIC Model Laws

The NAIC has three model laws governing data privacy: *Health Information Privacy Model Act* (Model #55); *NAIC Insurance Information and Privacy Protection Model Act* (#670) and *Privacy of Consumer Financial and Health Information Regulation* (#672), each of which is based upon or influenced by federal privacy laws. The NAIC's Model #670 contains many of the consumer rights found in these comprehensive state laws, which can be traced back to the Fair Credit Reporting Act (FCRA). ~~And~~ Model #672 is based, in large part, on GLBA and the HIPAA regulations. Generally, insurers and other entities licensed by state departments of insurance are exempted from many of these ~~carved out of more~~ comprehensive state privacy laws~~ of general applicability~~. Because of this, insurance regulators

must be aware when new protections are added to laws applicable to other businesses, especially when they address new technologies and ways consumer information is collected and shared, so that comparable protections can be added, as necessary, to the laws governing the insurance industry. Of note, GLBA and HIPAA each set a federal floor for the entities within their scope, from which states can build upon. This is what the NAIC did in drafting the *Health Information Privacy Model Act* (Model #55) and the *Privacy of Consumer Financial and Health Information Regulation* (#672). GLBA applies to the entire insurance industry, while HPAA applies to the health insurance sector.

A. NAIC Insurance Information and Privacy Protection Model Act (Model #670)

The NAIC adopted the *NAIC Insurance Information and Privacy Protection Model Act* (#670) in 1980 following federal enactment of the Fair Credit Reporting Act in 1970 and the Federal Privacy Act in 1974. This model act establishes standards for the collection, use and disclosure of information gathered in connection with insurance transactions by insurance companies, insurance producers and insurance support organizations.

A key aspect of this model is that it establishes a regulatory framework for consumers to: (1) ascertain what information is being or has been collected about them in connection with insurance transactions; (2) obtain access to such information for the purpose of verifying or disputing its accuracy; (3) limit the disclosure of information collected in connection with insurance transactions; and (4) obtain the reasons for any adverse underwriting decision.

This regulatory framework is facilitated through a requirement that insurers or agents provide a written notice to all applicants and policyholders regarding the insurer's information practices. The notice must address the following: (1) whether personal information may be collected from persons other than the individual or individuals seeking insurance coverage; (2) the types of personal information that may be collected, the ~~types of~~ sources and investigative techniques that may be used to collect such information; (3) the types of disclosures allowed under the law; (4) a description of the rights established under the law; and (5) notice that information obtained from a report prepared by an insurance support organization may be retained by the insurance support organization and disclosed to other persons.

Of note, the model prohibits disclosure of any personal information about an individual collected or received in connection with an insurance transaction without the individual's written authorization, subject to limited exceptions. However, some categories of information may be disclosed for marketing purposes if the consumer "has been given an opportunity to indicate that he or she does not want personal information disclosed for marketing purposes and has given no indication that he or she does not want the information disclosed." It also provides consumers with the right to request that an insurer provide access to recorded personal information, disclose the identity of the third parties to whom the insurance company disclosed information (if recorded); disclose the source of collected information (if available); and provide procedures by which the consumer may request correction, amendment, or deletion of recorded personal information.

Seventeen states have adopted Model #670: AZ, CA, CT, GA, HI, IL, KS, MA, ME, MN, MT, NV, NJ, NC, OH, OR, and VA.

B. NAIC Health Information Privacy Model Act (Model #55)

The NAIC adopted the *Health Information Privacy Model Act* (Model #55) following federal adoption of the privacy regulations authorized by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

This model sets standards to protect health information from unauthorized collection, use and disclosure by requiring insurance companies to establish procedures for the treatment of all health information by all insurance carriers. The drafters of Model #55 believed it was important that the same rules apply to all lines of insurance, since health

insurance carriers are not the only ones that use health information to transact their business. For example, health information is necessary for life insurance underwriting, and often essential to property and casualty insurers in settling workers' compensation claims and personal injury liability claims. Reinsurers also use protected health information to write reinsurance.

The model requires carriers to develop and implement written policies, standards, and procedures for the management of health information, including to guard against the unauthorized collection, use or disclosure of protected health information. It provides consumers with the right to access their protected health information and amend any inaccuracies. The model also requires insurers to obtain written authorization ~~("opt-in")~~ before collecting, using, or disclosing protected health information, except when performing limited activities.

Commented [CR1]: The language should clarify language to mean opt in

Many of the provisions found in Model #55 were later incorporated into the *Privacy of Consumer Financial and Health Information Regulation* (Model #672).

The following 13 jurisdictions have adopted legislation related to Model #55: CA, CO, DE, KY, LA, ME, MO, ND, RI, SD, TX.

C. NAIC Privacy of Consumer Financial and Health Information Regulation (Model #672)

The NAIC adopted the *Privacy of Consumer Financial and Health Information Model Regulation (Model #672)* in 2000. The model regulation was drafted to implement the requirements set forth in Title V of GLBA. GLBA imposed privacy and security standards on financial institutions, defined to include insurers and other insurance licensees, and directed state insurance commissioners to adopt certain data privacy and data security regulations. The provisions governing protection of financial information are based on privacy regulations promulgated by federal banking agencies. The model also contains provisions governing protection of health information that were taken directly from Model #55 and from the HIPAA Privacy Rule promulgated by HHS.

The model regulation provides protection for financial and health information about consumers held by insurance companies, agents, and other entities engaged in insurance activities. In general, the model regulation requires insurers to: (1) notify consumers about their privacy policies; (2) give consumers the opportunity to prohibit the sharing of their protected financial information with non-affiliated third parties; and (3) obtain affirmative consent from consumers before sharing protected health information with any other parties, affiliates, and non-affiliates.

The key difference between the treatment of financial information and health information is that insurers must give consumers the right to "opt out" of the disclosure or sharing of their financial information but insurers must obtain explicit authorization from the consumer ("opt-in") before sharing health information. Every jurisdiction has a version of this model regulation, although nineteen jurisdictions have only adopted the provisions regarding financial information and not the provisions regarding health information. Some jurisdictions that have adopted Model # 670 have adopted additional provisions from Model # 672 by bulletin rather than regulation.

IV. Summary of Health Insurance Portability and Accountability Act (HIPAA)

In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA), which, among other things, authorized the U.S. Department of Health and Human Services (HHS) to promulgate regulations governing the protection of consumer ~~privacy protections~~health information. The HIPAA Privacy Rule was finalized in 2000. ~~The rule~~ , and applies to covered entities, which are health plans ~~and~~, health care providers, and clearinghouses, and their business associates that conduct certain transactions on their behalf. The HIPAA Privacy Rule provides sets forth

restricting the permitted uses and disclosures of protected health information. HIPAA preempts state law unless only to the extent that thea state law provides more privacy protections for a consumer. covered entity or business associate would find it impossible to comply with both the state and federal requirements.

HIPAA provides individuals the right to access and amend their protected health information, the right to request the restriction of on uses and disclosures of protected health information, and the right to receive an accounting of disclosures made to other entitiesfor certain purposes.

A covered entity must obtain the individual's written authorization for any use or disclosure of protected health information unless it isthat is not for treatment, payment or health care operations of the covered entity, or otherwiseas permitted or required by the law, or for other specific purposes as outlined in the HIPAA Privacy Rule at 45 CFR 164.502. A covered entity is also required to provide notice of its privacy practices.

V. Summary of General Data Protection Regulation (GDPR)

The GDPR became effective in May 2018 and applies to U.S. companies if they collectare controllers or processors of personal data of data subjects within the E.U.from citizens of the E.U. over the internet. It requires companies (data "controllers") to obtain explicit consent from consumers to collect their data ("opt in") with an explanation of how the data will be used. It also contains standards for safeguarding the data collected. Under the GDPR, a consumer has the following rights: (1) to receive information about the processing of personal data; (2) to obtain access to the personal data; (3) to request that incorrect, inaccurate or incomplete personal data be corrected; (4) to request that personal data be erased when it is no longer needed or if processing it is unlawful; (5) to object to the processing of personal data for marketing purposes or on grounds relating to a consumer's particular situation; (6) to request the restriction of the processing of personal data in specific cases; (7) to receive personal data in a machine-readable format and the ability to send it to another controller ("data portability"); and (8) to request that decisions based on automated processing concerning the consumer or significantly affecting the consumer and based on consumer's personal data, are made by human beings.

VI. Summary of Recently Adopted Consumer Privacy Protection Laws

A. California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)

In 2018, California became the first U.S. state to adopt a comprehensive privacy law, imposing broad obligations on businesses to provide consumers with transparency and control of their personal data. The California Consumer Privacy Act (CCPA) became effective in 2020. Since it was adopted, it was amended by the California Privacy Rights Act (CPRA), which becomes effective Jan. 1, 2023. Additionally, the California Attorney General promulgated implementing regulations in 2020.

Scope

The CCPA, as amended by the CPRA (California law) applies to companies doing business in California that collect or process consumers' personal information and meet one of the following thresholds: (1) has annual gross revenue in excess of $25,000,000 in the preceding calendar year; (2) annually buys, sells, or shares the personal information of 100,000 or more consumers or households; or (3) derives 50% or more of its annual revenue from selling or sharing consumers' personal information.

Exemptions

The law does not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (GLBA), and its implementing regulations. CCPA also includes an exemption for protected health

information governed by the HIPAA Rules as well as ~~It also does not apply to protected health information that is governed by the privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services (HHS). Furthermore, this law contains~~ an entity-level exemption for HIPAA-covered entities or business associates ~~governed by the privacy, security, and breach notification rules issued by HHS~~.

Consumer Rights

California law provides consumers with the following rights : (1) to request deletion of any personal information;[1] (2) to correct inaccurate personal information, taking into account the nature of the personal information and the purposes of the processing of the information; (3) to know about and access the personal information being collected by requesting that the business disclose: the categories and specific pieces of personal information collected, the categories of sources the information was collected from, the business purpose for collecting the information, the categories of third parties with whom the information is shared, and the specific pieces of personal information that was shared; (4) to request the personal information provided by the consumer in a format that is easily understandable, and to the extent technically feasible, in a structured, commonly used, machine-readable format that may also be transmitted to another entity at the consumer's request without hindrance; (5) to know what personal information is sold or shared and to whom; (6) to opt out of the sale or sharing of personal information; (7) to limit the use and disclosure of sensitive personal information; and (7) to not be retaliated against for requesting to opt out or exercise other rights under the law.

Business Obligations

The law imposes the following obligations on all covered businesses: (1) prohibits retaining a consumer's personal information for longer than reasonably necessary for the disclosed purpose; (2) requires implementing reasonable security procedures and practices; (3) requires notice of the following: collection of personal information, including sensitive personal information, retention of information, right to opt out of sale and sharing, and financial incentives; (4) prohibits using sensitive personal information when a consumer has requested not to use or disclose such data.

Enforcement

The CPRA amends the CCPA by placing administrative enforcement authority with the California Privacy Protection Agency, a new state agency created by the CPRA. Under the CPRA, the attorney general retains authority for seeking injunctions and civil penalties. Additionally, if personal information is breached, the consumer can pursue a private civil action against the company.

B. Colorado Privacy Act (CPA)

Scope

The Colorado Privacy Act (CPA) takes effect on July 1, 2023. It applies to entities that conduct business in Colorado or produce or deliver commercial products or services intentionally targeted to residents of Colorado and satisfy one of the following thresholds: (1) controls or processes the personal data of 100,000 or more consumers in a year; or (2) derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of 25,000 or more consumers. The law defines "controllers" as those that "determine the

[1] ~~And even when~~When information is "deleted," the CCPA right to deletion allows the business to "maintain a confidential record of deletion requests solely for the purpose of preventing the personal information of a consumer who has submitted a deletion request from being sold, for compliance with laws or for other purposes."

purposes for and means of processing personal data" and defines "processors" as those that "process data on behalf of a controller."

Exemptions

The law contains data-based exemptions (rather than entity-level exemptions) for protected health information collected, processed, or stored by HIPAA-covered entities and their business associates, and information and documents created by a HIPAA-covered entity for purposes of complying with the HIPAA Rules~~and its implementing regulations~~. Additionally, the law contains an exemption for any personal data collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act (GLBA), and implementing regulations, if such collection, processing, sale, or disclosure is in compliance with that law.

Consumer Rights

The CPA provides consumers with the following rights: (1) to opt out of targeted advertising, sale of personal data, and profiling; (2) to confirm whether a controller is processing the consumer's personal data and the right to access such data; (3) to correct inaccuracies in personal data; (4) to delete personal data; and (5) to obtain the personal data in a portable and readily usable format that allows the consumer to transmit the data to another entity.

Business Obligations

The CPA imposes affirmative obligations on controllers, including the following: (1) provide consumers with an accessible, clear, and meaningful privacy notice; (2) specify the express purposes for which personal data are collected and processed; (3) collection of personal data must be adequate, relevant and limited to what is reasonably necessary in relation to the specified purposes; (4) not process personal data for purposes that are not reasonably necessary to or compatible with the specified purposes, without obtaining consent from the consumer; (5) take reasonable measures to secure personal data; (6) not process personal data in violation of any law that prohibits unlawful discrimination; and (7) not process a consumer's sensitive data without first obtaining the consumer's consent. Additionally, controllers are required to enter into contracts with data processors, referencing the responsibilities under the CPA and controllers must conduct a data protection assessment prior to any processing activities that have a heightened risk of harm to consumers.

Enforcement

The CPA does not contain a private right of action but provides the state attorney general and district attorneys authority to take action against entities for violations.

C. Virginia Consumer Data Protection Act (CDPA)

Scope

The Virginia Consumer Data Protection Act (CDPA) becomes effective Jan. 1, 2023. It applies to entities that conduct business in Virginia or produce products or services targeted to Virginia residents when they control or process personal data of at least 100,000 consumers or control or process personal data of at least 25,000 consumers and also derive over 50% of gross revenue from the sale of personal data.

Exemptions

The law contains entity-level exemptions for those subject to GLBA and HIPAA. It specifically exempts financial institutions and data subject to GLBA, and covered entities or business associates governed by the HIPAA Rules.

~~privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services. It also exempts protected health information under HIPAA.~~

Consumer Rights

The CDPA provides consumers with the following rights: (1) to confirm whether or not a controller is processing the consumer's personal data and if so, to provide the right to access such personal data; (2) to correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of processing of the consumer's personal data; (3) to delete personal data provided by or obtained about the consumer; (4) to obtain a copy of the consumer's personal data in a portable and readily usable format that allows the consumer to transmit the data to another controller; and (5) to opt out of the processing of the personal data for purposes of targeted advertising, sale of personal data, and profiling.

Business Obligations

Under the law, controllers have the responsibility to do the following: (1) limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed; (2) not process personal data without consumer consent for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such personal data is processed; (3) establish, implement, and maintain reasonable data security practices to protect personal data; (4) not process personal data in violation of any laws that prohibit unlawful discrimination against consumers and not discriminate against consumers exercising their rights under this law; and (5) not process sensitive data concerning a consumer without obtaining the consumer's consent. In addition, controllers must provide consumers with a reasonably accessible, clear, and meaningful privacy notice. Processing activities undertaken by a processor on behalf of a controller must be governed by a data processing agreement. Controllers also must conduct data protection assessments that evaluate the risks associated with processing activities.

Enforcement

Similar to the Colorado law, the law does not contain a private right of action but provides the state attorney general authority to pursue action against entities for violations.

VII. Summary of Working Group Discussions of Selected Key Points

The working group began discussions Dec. 8, 2019, during the Fall National Meeting with the following minimum consumer privacy protections being considered as appropriate for the business of insurance. These rights were based on the Working Group's proposed 2020 charges and are included in the Working Group's initial 2019 Work Plan:

1. the right to receive notice of an insurer's privacy policies and practices;
2. the right to limit an insurer's disclosure of personal data;
3. the right to have access to personal data used by an insurer;
4. the right to request the correction or amendment of personal data used by an insurer;
5. the right of data ownership; and
6. the right of data portability.

The Work Plan also said that the Working Group discussions would focus on data privacy (rather than data security) and identify areas within NAIC models and state requirement where consumer data privacy protections might need to be enhanced due to changes in technology. In her Dec. 8 presentation, Jennifer McAdam (NAIC) outlined existing privacy provisions in NAIC models and state insurance laws. She said the difference between data privacy and data

Commented [CR2]: BCBSA recommends that the PPWG include a footnote to clarify, as the chair has stated, that these are not "rights", but are rather "issues" or "rights to request". This will help avoid confusion.

security is that data privacy is about how data is being collected and used by businesses; while data security is about how data that a business has already collected and has in its possession~~)~~ is stored and protected from unauthorized access. She said the two are often conflated and there are some laws that address both – like GDPR, for example. Furthermore, as many comments have noted, the two issues overlap because a breach of security often results in a loss of privacy. Ms. McAdam said the CCPA is an example of a data privacy law that governs how businesses collect and use consumer data; the rights consumers have to know how that data is being used; the rights consumers have to challenge the accuracy of the data; and how it is being used. Data privacy laws are focused on legal protections for data and consumer rights.~~:~~ In comparison, data security laws, such as the NAIC's Insurance Data Security Model Law (#668), require operational and technological protections sufficient to ensure that the legal protections are meaningful. Ms. McAdam explained that Model #668 governs how businesses protect the data once it has been collected as well as what businesses need to do if those protections fail as the result of a data breach or other cybersecurity event.

State insurance regulators were concerned about the consumer data that insurers were already presenting in rate filings that had ballooned up to thousands of pages of different data points being gathered by insurers on consumers. They have also seen an increased reliance on third-party risk scores that aggregate consumer information in order to make determinations and conclusions about that information. Regulators noted that insurers have a responsibility to ensure that the third parties used are following state laws and complying with the state's standards for accuracy and fairness. In addition to disclosing the identity of ~~providing disclosure of the~~ third parties used by insurers when consumers request it, insurers are required to report how the information was gathered; where it was drawn from (e.g., web traffic, geolocation data, social media, etc.); and why the company thinks it needs to use those particular data points as the possibilities available to insurers are endless.

Industry asked the Working Group to consider: 1) Workability by allowing for various exemptions for operational and other reasons that acknowledge vital business purposes for insurers to collect, use, and disclose information. For example, Article IV of the NAIC Model #672 was developed to implement the GLBA, and the exceptions embedded into Section 13 of Model #672 are instructive as to the types of operational functions that need to be preserved and facilitated; 2) Exclusivity by avoiding dual regulation, so insurers are not simultaneously subject to potentially inconsistent or conflicting interpretations by more than one regulator; 3) Clarity by asking that care be taken to consider how best to dovetail with existing models/ laws/regulations; consulting other resources and educating legislators on how privacy bill language impacts the insurance industry, including the legal requirements to retain and use certain data, as well as data mandates; 4) an effective date that allows advance time (like the two to five years that was afforded under the GDPR) for insurers to be ready for implementation, to avoid having piecemeal revisions like the CCPA and the GDPR, as well as a roll-out period with different dates for different provisions within that time frame as a more measured approach to undertake such a significant endeavor.

Consumer Representatives asked the Working Group to consider that: 1) Data vendors are scraping personal consumer information from public sources to produce consumer profiles, scores, and other tools for insurers. The data vendor products, while assembled from public information, raise concerns over consumers' digital rights and privacy; 2) Many data vendors and many types of personal consumer information are not subject to FCRA consumer protections. In turn, many of the types of data and algorithms used by insurers are not subject to either FCRA consumer protections (even though they are the functional equivalent of a consumer report) or the NAIC model law/regulation protections; 3) It is unclear whether the NAIC models cover the new types of data being generated by consumers as part of, or related to, insurance transactions. For example, consumers are producing large volumes of data through telematics programs from devices collecting personal consumer data in the vehicle or home or through wearable devices; 4) There are a lots of organizations working on consumer digital rights (such as the Center for Digital Democracy, the Electronic Privacy Information Center, the Electronic Frontier Foundation, the Public Knowledge-Privacy Rights Clearinghouse, the Public Citizen, the U.S. Public Interest Research Group, and the World Privacy Forum) from whom

input and presentations at Working Group meetings should be solicited; and 5) If consumer disclosures are to be used, that the disclosure should be a compliance or enforcement tool that would be created using consumer focus testing and established best practices for the creation of such consumer disclosures.

The COVID-19 pandemic slowed down the Working Group's discussions in 2020; however, discussions continued through seven virtual meetings and two regulator-only meetings of subject matter experts as areas of concentration were being narrowed leading to the Working Group requesting additional guidance from its parent committee.

In April 2021, the Working Group's discussions were redirected to six consumer data privacy rights or types of consumer data privacy protections based on the specific examples identified in item 1.c. of the NAIC Member Adopted Strategy for Consumer Data Privacy Protections received through its parent Committee, the Market Regulation and Consumer Affairs (D) Committee. The Working Group's task was to comment on the following consumer privacy rights concerning consumers' personal information as a basis for a privacy protection framework for the insurance industry (not just health insurance):

1. Right to opt out of data sharing;
2. Right to limit data sharing unless the consumer opts in;
3. Right to correct information;
4. Right to delete information;
5. Right to data portability;
6. Right to restrict the use of data.

Consequently, the Working Group was also tasked with analyzing or determining how insurers were protecting these rights – either to comply with state or federal statutory or regulatory requirements, or on their own initiative or through the adoption of voluntary standards. In 2021, the Working Group met ten times and the regulator only subject matter experts met nine times.

Prior to the 2021 Summer National Meeting, Working Group discussions focused on discussion of, and input on, the following key points from regulators, industry, and consumers for each of the six consumer privacy data rights noted above: definition; examples; consumer risk/impact; current state and federal laws/rules; insurer/licensee impact; actions necessary/insurer obligations to minimize consumer harm; and recommendations. Suggestions that separate privacy requirements be established for each line of business were discussed, but there was consensus that they did not seem to be feasible, as different consumer data privacy requirements across lines of business would limit both consumer protections and understanding.

It was noted during Working Group discussions that insurers utilize third party vendors as sources of data collection and that such vendors may not be subject to regulation by state insurance departments. Regulators stated that the insurers they regulate bear the responsibility for compliance with state insurance privacy requirements. Insurers felt they could not be held responsible because they did not know how such vendors collected or used consumer data and had no way to control the vendors business activities. Regulators and consumer representatives expressed different opinions indicating that insurers' contracts with such vendors could and should be written to require vendors and insurers maintain compliance with insurance regulations regarding consumer data privacy.

During the 2021 Summer National Meeting, NAIC members further recommended that the Working Group's discussion be expanded to include the issue of consumer data ownership.

Working Group discussions revealed that state insurance regulators and consumer representatives believe consumers own the data that is collected and used by the insurance industry to market, sell, and issue insurance policies. It was felt that the type of data collected (name, age, date of birth, height, weight, income, physical condition, personal habits, etc.) describes who a person is and distinguishes one person from another by its very nature. When a consumer shares

their data with an insurance company, it is with the understanding that the consumer is letting the company borrow it for a time to determine what insurance rates and insurance coverage the consumer needs. The consumer is not giving up their data to an insurer so it can be sold or given to other organizations from whom the consumer is not seeking insurance coverage, or any other product. Consumer representatives indicated that this practice had happened when they did an online search for insurance rates on health plans. As a result, the consumer representative received hundreds of cold calls from companies selling products other than insurance. When the consumer representative asked with whom the insurance company shared his data, the company sent him a list of 1,700 companies – none of which sold insurance.

The privacy policy statement in Appendix A is designed to be the foundation for the minimum consumer data privacy protections that are appropriate for the business of insurance to be applied to NAIC model #672 as revisions. It is intended to kick start the next step in creating revisions by defining the parameters of the existing consumer data privacy rights; by suggesting definitions and by showing examples of consumer risks. Further discussion is necessary, however, to clarify consumer data privacy rights that may not be fully protected in federal laws or fully covered under NAIC Model laws, and to decide how to provide appropriate protections.

VIII. Conclusion and Recommendations

Months of detailed discussions with regulator, industry, and consumer stakeholders, and the comments they have submitted, have led the Working Group to determine that the *NAIC Insurance Information and Privacy Protection Model Act (Model #670)* and the *Privacy of Consumer Financial and Health Information Regulation (Model #672)* have in the past provided an effective regulatory framework for consumer privacy protections to oversee and enforce consumer data privacy as required by state and federal statutes and regulation. However, these models were adopted by the NAIC 20 and 40 years ago, respectively; with only 17 jurisdictions adopting Model #670.

In consideration of the many changes that have occurred in recent years, as well as the rate of increase in the use of new technologies (AI, machine learning, accelerated underwriting, rating algorithms, etc.), and big data by insurers, the Working Group recommends that models 670 and 672 be amended to ensure that regulators can continue to provide consumer data privacy protections essential to meet the consumer data privacy challenges presented by the public use of technology and data by insurers in today's business environment.

The Working Group also recommends the NAIC's Market Regulation Handbook be updated, as necessary, to provide guidance to state insurance regulators so they can verify insurers' compliance the regulatory framework for consumer privacy protections.

Commented [CR3]: NAIC should clarify the process on how Model laws will be amended in context of federal privacy laws and also when new data elements are added.

Commented [CR4]: BCBSA encourages the working group to focus its revisions on Model #672. The working group indicated in a previous meeting that Model #672 would be the foundation for its work. Further, Model #670 has not been accepted as broadly throughout the states as Model #672.

Appendix A

National Association of Insurance Commissioners
Policy Statement on Consumer Data Privacy Protections

Because the business operations of insurance companies are dependent upon the collection and use of personal information and data, state insurance regulators have long understood the need to balance an insurance company's need to collect consumer information and data with the consumer's right to limit the collection and use of data.

The NAIC adopted the *Insurance Information and Privacy Protection Model Act* (Model #670) in 1980 to establish standards for the collection, use and disclosure of information gathered in connection with insurance transactions. A key aspect of this model is that it establishes a regulatory framework for consumers to (1) ascertain what information is being or has been collected about them in connection with insurance transactions; (2) obtain access to such information for the purpose of verifying or disputing its accuracy; (3) limit the disclosure of information collected in connection with insurance transactions; and (4) obtain the reasons for any adverse underwriting decision. This regulatory framework is facilitated through a requirement that insurers or agents provide a written notice to all applicants and policyholders regarding the insurer's information practices.

The NAIC adopted the *Privacy of Consumer Financial and Health Information Model Regulation* (Model #672) in 2000. The model regulation was drafted to implement the requirements set forth in Title V of the federal *Gramm-Leach-Bliley Act* (P.L. 106-102) of 1999 (GLBA). GLBA imposed privacy and security standards on financial institutions and directed state insurance commissioners to adopt certain data privacy and data security regulations. The model also contains provisions governing protection of health information that were taken directly from the Health Insurance Portability and Accountability Act Privacy Rule promulgated by HHS. The NAIC model regulation requires insurers to: (1) notify consumers about their privacy policies; (2) give consumers the opportunity to prohibit the sharing of their protected financial information with non-affiliated third parties; and (3) obtain affirmative consent from consumers before sharing protected health information with any other parties, affiliates, and non-affiliates. The key difference between the treatment of financial information and health information is that insurers must give consumers the right (with limited exceptions) to "opt out" of the disclosure or sharing of their financial information, but insurers must get explicit authorization ("opt in") before sharing health information.

Commented [CR5]: This is inconsistent with HIPAA's TPO exception and need to be recognized for HIPAA entities of existing law

This policy statement is based on the consumer protections set forth in these two models and serves the purpose of informing licensed insurance entities, consumers, and the other state and federal regulatory agencies on what the NAIC currently supports as the minimum consumer data privacy protections that are appropriate for the business of insurance. The policy statement is not intended to modify any existing NAIC models and does not carry the weight of law or impose any legal obligations in states that have adopted those models.

The policy statement addresses consumer data privacy protections of (1) transparency; (2) consumer control; (3) consumer access; (4) data accuracy; and (5) data ownership and portability. The policy statement intentionally excludes standards for data security and standards for the investigation and notification to an insurance commissioner of a licensed insurance entity's cybersecurity event, which are the subject of separate model laws and interpretive guidance.

The following definitions are used for the purposes of this policy statement.

A. "Adverse Decision" means declination of insurance coverage, termination of insurance coverage, charging a higher rate for insurance coverage, or denying a claim.
B. "Consumer" means an individual who is seeking to obtain, obtaining, or have obtained a product or service from

an insurer. For example, an individual who has submitted an application for insurance is a consumer of the company to which he or she has applied, as is an individual whose policy with the company has expired.

C. "Customer" means a consumer with whom an insurer has an on-going relationship.

D. "Licensee" means any insurer, producer, or other person licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to a state insurance law.

E. "Personal Information" means any individually identifiable information or data gathered in connection with an insurance transaction from which judgments can be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit, health, or any other personal characteristics. Personal information includes:

1. "Non-Public Personal Information," which means information that a consumer provides to a licensee to obtain an insurance product or service (like income, credit history, name and address); information about a consumer a licensee has as a result of a transaction involving an insurance product or service (like premium payment history, how much a life insurance policy is worth, and the value of personal property insured); and all other information about a consumer that a licensee uses in connection with providing a product or service to a consumer.
2. "Non-public personal health information," which means any information that identifies a consumer in some way, and includes information about a consumer's health, including past and present physical and mental health, details about health care, and payment for health care.

I. Transparency

A licensee should provide a clear and conspicuous notice to consumers that accurately reflects its privacy policies and practices when it first requests personal information about the consumer from the consumer or a third party.

A licensee should also provide a periodic notice of its privacy policies and practices to customers not less than annually during the continuation of the customer relationship.

If a licensee makes an adverse decision based on information/data that was not supplied by the consumer, the licensee should provide the consumer with the specific reasons for the adverse decision.

II. Consumer Control

Licensees should, at a minimum, provide consumers the opportunity to prohibit the sharing of their non-public personal information with third parties, except for specific purposes required or specifically permitted by law including HIPAA for HIPAA covered entities.~~.~~ (Opt-Out)

~~Licensees should obtain affirmative consent from consumers before sharing non-public personal health information with any other entity, including its affiliates and non-affiliates.~~ (Opt-In)

III. Consumer Access

Any consumer should have the right to submit a request to a licensee to obtain access to his/her personal information used by the licensee in its operations. Upon request, the licensee should within 30 business days provide a copy of the consumer's personal information, an explanation on how the personal information was used (i.e., rating, underwriting, claims), and provide the source of the personal information. If personal information is in coded form, the licensee should provide an accurate translation in plain language.

Commented [CR6]: BCBSA recommends adoption of this as it is consistent with HIPAA

Commented [CR7]: The opt-in provision is inconsistent with HIPAA

IV. Data Accuracy

Within 30 business days after receiving a request from a consumer to correct, amend, or delete personal information used by the licensee in its operations, the licensee should either make the requested correction, amendment, or deletion or notify the consumer of its refusal to do so, the reasons for the refusal, and the consumer's right to file a statement of dispute setting forth what the consumer thinks is the correct information and the reasons for disagreeing with the licensee.

For HIPAA covered entities, this provision shall align with HIPAA requirements and shall be exempt from additional requirements as specified. For Non-HIPAA entities, if the licensee corrects, amends, or deletes personal information, the licensee should notify any person or entity that has received the prior personal information within the last 7 years. If the licensee does not correct, amend, or delete the disputed personal information, the licensee should notify any person or entity that has received the prior personal information within the last 7 years of the consumer's statement of dispute.

Commented [CR8]: Under HIPAA, a covered entity has to notify of an amendment if the individual requests a specific person/entity or if the covered entity knows an entity could rely on the information.

V. Data Ownership and Portability

A customer should have the right to request a copy of his/her personal information that he/she has provided to the licensee for use in the licensee's operations. A licensee should provide a customer a copy of his/her personal information within 30 business days of the request. ~~Examples of this type of personal information include telematics data and "Internet of Things" ("IoT") data.~~

Commented [CR9]: This exam is too broad.

DATE: November 29, 2021

TO: Chair Amann, Vice Chair Kreiter, Members of the Privacy Protections WG, & Lois Alexander

FROM: NAIC 2021 Consumer Representatives Brenda Cude & Karrol Kitt

Thank you very much for the opportunity to provide comments on the Final Exposure Draft of the Report on Consumer Data Privacy to the D Committee Privacy Protections Working Group. We appreciate the work of the NAIC Privacy Protections Working Group to develop the Report and the included Privacy Policy Statement. We also appreciate this opportunity to provide comments on the final exposure draft of the WG. We agree with insurers that it is important that consumers have a right to know the personal information that companies maintain about them. We respectfully submit the following thoughts to the Working Group on the final draft of the report.

To expedite this final comment opportunity, we will provide the Report page number and identify the paragraph/section that the comment refers to. Our comments begin with page 9 of the Report.

Page 9:

Last Paragraph: – It is Important to distinguish the difference between data privacy and data security for this Report and retain the focus on data privacy.

Page 10:

First Full Paragraph - As you state, the amount of information provided by insurers has expanded greatly and state regulators are challenged to keep pace with this expansion. What might have been a manageable task has turned into a monumental task. The amount of information from third-party sources that insurers now use in their rate filings has contributed to this challenge.

Second & Third Paragraphs: - We support these two paragraphs which provide the contrast of Industry and Consumer Representatives' perspectives regarding privacy features.

Page 10:

First Line/Paragraph on Page: - We think describing these as issues related to data privacy would be appropriate, perhaps with a note that they were initially described as rights.

Third Paragraph: - We support retaining this paragraph as insurer use of data from third-party vendors is an important consumer issue related to data privacy.

Fourth Paragraph: - It is important that consumers know how insurers use the information they provide to them. We seriously doubt whether most consumers understand that the information they provide to the insurer is used to determine insurance rates and the coverage offered to them.

Page 12:

First Paragraph: - It would be disappointing if this is an endorsement of consumers receiving only minimum consumer data privacy protections. With all the work the Working Group has done this year, a "basement" level foundation is disappointing.

2nd *Paragraph*: - We are told by industry that new products and new ways of selling and servicing those products are to be expected as the insurance industry evolves. We also would argue that

the same applies to consumer privacy protections. Since the Models now utilized for Privacy Protections are 20 to 40 years old, it is past-time to modernize the standards, how they are communicated to consumers, and how they are implemented.

Page 13:

First Paragraph: - A balance between the insurers' need to collect and use consumer data and the consumers' right to limit the collection and use of their data is essential. In the past, that balance was absent, with greater emphasis on the insurers' need for consumer data.

Third Paragraph: - This difference between the approach to privacy protections for financial and health information is in the out-in vs. opt-out approaches. In the opt-out approach, the responsibility is placed on the consumer to maintain data privacy. In the opt-in approach, the industry has more responsibility. We support the opt-in approach, shifting more of the responsibility to the industry.

Page 14

Definition C: - We recommend adding a definition of "on-going relationship." We assume there is an on-going relationship as long as a consumer has a policy with an insurer. But is there an on-going relationship if a consumer applies for and decides not to purchase a policy? Is there an on-going relationship after a consumer cancels a policy?

Transparency Section, 1st Paragraph: - We strongly urge further specific standards be provided to clarify what it means for a disclosure to be "clear and conspicuous." One way to establish that a disclosure is "clear and conspicuous" would be through consumer testing. Or, there might be other specific standards that address reading levels, font sizes, etc.

Transparency Section, 2nd Paragraph: - Consumers should be given specific reasons for an adverse decision, rather than a general blanket statement providing generic information. As an example: rather than stating that a credit score is too low, the consumer could be told that their credit score of 585 is below the acceptable 650 credit score. In another example, rather than stating that the applicant's annual income is too low, they could be told that their $50,000 annual income is less than $75,000.

In conclusion, we pledge to continue to support any work on Privacy Protections in 2022.

Insurance Privacy Protection: Do the "Right" Thing

A Consumer Perspective

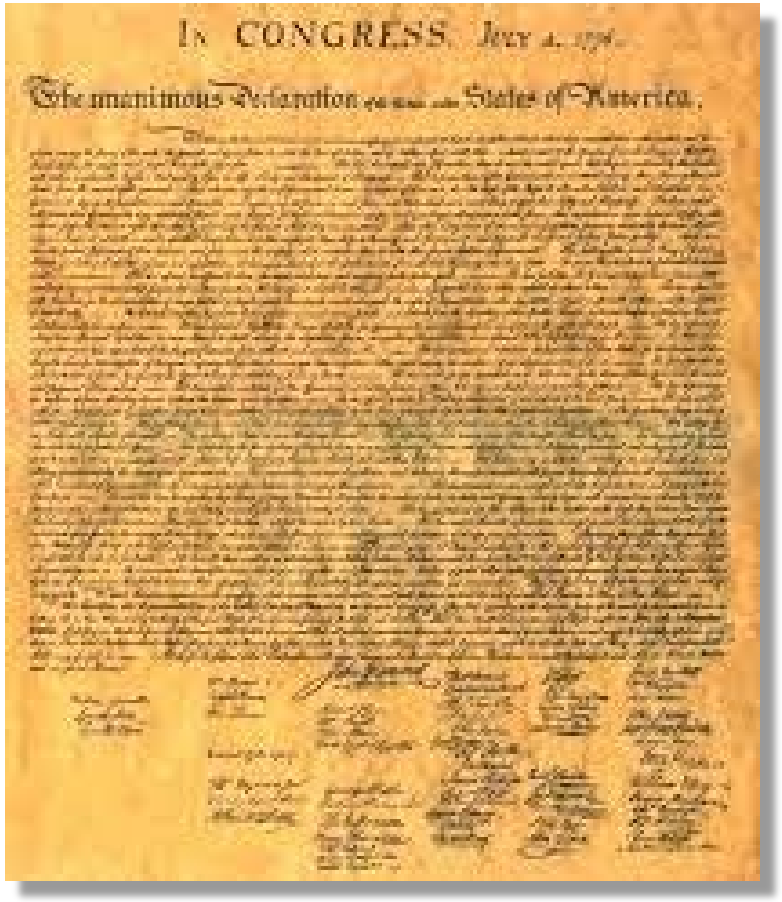
Presented to the NAIC Consumer Liaison Committee
December 13, 2021

Harold M. Ting, PhD
NAIC Consumer Representative

Privacy Protection (D) WG 2021 Charges

- What "rights" should consumers have
  - *Opt out of data sharing*
  - *Opt in of data sharing*
  - Correct information
  - Delete information
  - Data portability
  - *Restrict use & collection of data*

Fundamental "Rights"


IN CONGRESS, July 4, 1776.

The unanimous Declaration of the thirteen United States of America,

"We hold these Truths to be self evident, that all Men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty, and the Pursuit of Happiness...."

Declaration of Independence

Fundamental Consumer Rights

- *Consumer rights should be defined by ethical principles*
- *Fair Information Principles that protect the privacy rights of consumers* [1]
- *NAIC needs its Fair Information Principles for the insurance industry as the basis for revising its model acts & regulations*

Code of Fair Information Practices, 1973 [2]

1. Openness - *personal data record-keeping should not be hidden*
2. Access - *people should be able to find out what info is collected & its use*
3. Secondary Use - *people should be able to prevent use of their info obtained for one purpose from being used or made available for other purposes without the person's consent.*
4. Correction – *people should be able to correct or amend an inaccurate record about them*
5. Security - *Organizations must assure the reliability of the data for their intended use & take precautions to prevent its misuse.*

Regulators Have Had to Update Principles

- Changes in technology & data practices
  - New & increasingly invasive technologies
  - Collection of personal data beyond what is needed
  - Uses of AI that can have unwanted consequences
  - Significant security breaches posing serious fraud risks
- Increasing consumer concerns about privacy

NAIC Models Are Outdated

- NAIC model laws & regulations
  - 1980: Insurance Information & Privacy Protection Model Act (#670)
  - 1998: Health Information Privacy Model Act (#55)
  - 2000: Privacy of Consumer Financial & Health Information Regulation (#672)
- Based on Fair Credit Reporting Act (1970), Federal Privacy Act (1974), HIPAA (1996)

Fair Information Principles Must Be Real-World Based

Corporate Privacy Policies Are Too Complex

- Pew Research Center survey of 4,272 adults in 2019 [3]
  - Adults don't understand company privacy policies
    - Only 9% of adults always read the privacy policy
    - When they read the policies, only 22% read them completely, before agreeing to their terms
  - 79% are concerned how companies use their information, especially data they do not wish to share
- Ipsos 2018 Global Advisor survey of over 1,000 U.S. adults [4]
  - 75% said they should be able to refuse to let companies collect their data
  - 66% would be more comfortable if their data were not shared or sold
  - 53% did not trust financial services companies to use their data "in the right way"

Companies Collect Excessive Data

- "Data collection has been the default habit for engineers & database architects for the past few decades….engineers tend to collect more data because they don't know if an AI model could potentially benefit from it in the future." Bessemer Venture Partners [5]

- A survey by Lewis & Ellis Actuaries and Consultants found that most insurance companies surveyed check social media sites during their underwriting process. Most use Google, and some check LinkedIn, Facebook, Instagram or Twitter. [6]

- Collecting data not needed for intended transactions facilitates use of hidden algorithms that may harm certain populations unintentionally or illegally. [7]

Personal Data
Is Poorly Protected on the Internet

1. Many Privacy Policies Don't Protect

- *"We may use cookies & other technologies such as web beacons and pixels to collect information about your online activities over time & across third-party websites or online services which may allow a third party to track your online activities over time & across different sites when you use the Websites."*

- *"The Websites may not respond to Do Not Track requests or headers from some or all browsers."*

Personal Data Is Poorly Protected on the Internet

2. ”Dark Pattern” interfaces subvert user intent [8]

- *“Facebook & Google have privacy intrusive defaults, where users who want the privacy friendly option have to go through a significantly longer process. They even obscure some of these settings so that the user cannot know that the more privacy intrusive option was preselected.”*
- *“The popups from Facebook, Google & Windows 10 have design, symbols & wording that nudge users away from the privacy friendly choices. Choices are worded to compel users to make certain choices, while key information is omitted or downplayed. None of them lets the user freely postpone decisions. Also, Facebook & Google threaten users with loss of functionality or deletion of the user account if the user does not choose the privacy intrusive option.”*

Personal Data Is Poorly Protected on the Internet

3. Internet of Things (IoT) Data Collection

- "U.S. patients may have little access to their raw data collected & held by device manufacturers in the United States under the HIPAA Privacy Rules." [9]
- FTC policy statement, 9/15/21: the 2009 Health Breach Notification Rule covers personal health info collected by digital apps & wearable devices.[10]

Data Breaches Are Inevitable

- Data breaches occur, no matter how diligent organizations are about data security
- Identity Theft Research Ctr statement to Senate Commerce Committee [11]
  - Publicly reported breaches through Sept 2021 (1,291) exceeded 2020 total by 17%
  - 160 million people affected In Q3 2021

Privacy Enforcement Capability is Poor [12]

- "Our current privacy laws are woefully out of date and fail to provide the necessary protections for our modern age. We also now face threats from foreign adversaries that target the personal data stored in U.S. companies and U.S. government agencies."
- "The FTC only has authority to bring enforcement actions against unfair and deceptive practices in the marketplace, and it lacks the ability to create prospective rules for data security."
- "The Consumer Financial Protection Bureau similarly lacks data protection authority and only has jurisdiction over financial institutions. Neither of these agencies possess the resources needed to address data security."

Fair Insurance Industry Information Principles: What I Deserve as a Consumer

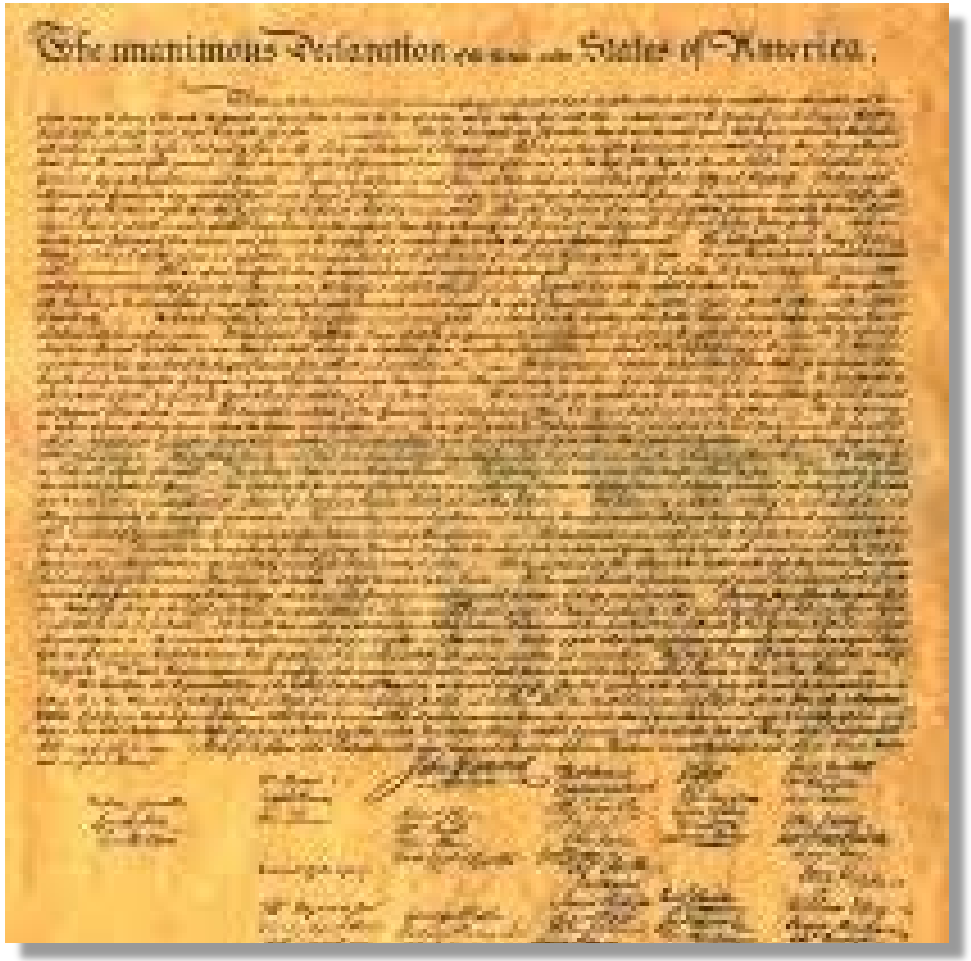
1. Notice - *of purpose and rights at time of collection*
2. Openness - *clear & periodic notice of privacy policies & practices, reasons for any adverse actions*
3. Collection - *data minimization (only data needed for transaction)*
4. Data quality - *keep relevant, accurate, up-to-date as long as used*
5. Use limitation - *only as needed for provision of insurance, except as permitted or required by law*
   - *ability to opt-out of sharing with affiliates, where not requested*
   - *Sharing with unrelated third parties prohibited unless consent given for specific parties*

Insurance Fair Information Principles (cont.)

6. Access - ability to obtain information in consumer-friendly formats & sources of data in reasonable time frames
7. Correction - *right to correct, amend, delete or add information where accuracy is legally disputed*
8. Data security - *protect all information linked to consumer through reasonable safeguards; delete or de-identify when no longer used*
9. Accountability - *appropriate penalties to incent compliance.*

In Summary

- Privacy protection should focus on protecting consumers
- Protections should be based on values & ethics
- NAIC needs to agree upon Fair Information Principles for the insurance industry
- Then apply those principles to revise its model laws & regulations



Endnotes

1. *Robert Gellman, "Fair Information Practices: A Basic History", Version 2.21, September 3, 2021, pp 44 45 at https://www.bobgellman.com/rg docs/rg FIPShistory.pdf*
2. *Electronic Privacy Information Center, "The Code of Fair Information Practices", at https://epic.org/fair-information-practices/*
3. *Pew Research Center, "Americans and Privacy: Concerned, Confused And Feeling Lack of Control Over Their Personal Information", November 15, 2019.*
4. *Ipsos, "Global Citizens & Data Privacy", World Economic Forum, Davos 2019 at https://www.ipsos.com/sites/default/files/global-citizens-data-privacy.pdf*
5. A. Ferrara, J. Schwerin and M. D"Onofrio, "How Data Privacy Engineering Will Prevent Future Data Oil Spills", Bessemer Venture Partners, Sept 2019.

Endnotes (cont.)

6. *Cameron Huddleston, "How Life Insurance Companies Get Intel on You", Forbes Advisor updated on Mar 26, 2021 at https://www.forbes.com/advisor/life insurance/personal data/ .*
7. Erin McCormick, "What happened when a 'wildly irrational' algorithm made crucial healthcare decisions", The Guardian, July 2, 2021, at https://www.theguardian.com/us news/2021/jul/02/algorithm crucial healthcare decisions
8. "Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy", NORWEGIAN CONSUMER COUNCIL (Jun. 27, 2018) at https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

Endnotes (cont.)

9. G. Cohen, S. Gerke, D.B. Kramer, “Ethical & Legal Implications of Remote Monitoring of Medical Devices”, The Milbank Quarterly, Oct. 2020.
10. M. Bellamoroso, ed. by A. Pyrinis, “FTC Signals Move Towards Tighter Data Privacy for Healthcare Apps”, Harvard Journal of Law & Technology Digest, Nov 6, 2021 at http://jolt.law.harvard.edu/digest/ftc signals move towards tighter data privacy for healthcare apps
11. Identity Theft Research Center, Identity Theft Resource Center to Share Latest Data Breach Analysis With U.S. Senate Commerce Committee, Oct 6,2021 at https://www.idtheftcenter.org/identity theft resource center to share latest data breach analysis with u s senate commerce committee number of data breaches in 2021 surpasses all of 2020/

Endnotes (cont.)

12. Electronic Privacy Information Center, ”Enforcement of Privacy Laws” at https://epic.org/issues/data-protection/enforcement-of-privacy-laws/

Related Information

Proposed Consumer Bill of Rights, Developed by US Department of Commerce 2012

1. INDIVIDUAL CONTROL *Consumers have a right to exercise control over what personal data companies collect from them & how they use it.*

2. TRANSPARENCY *Consumers have a right to easily understandable & accessible information about privacy & security practices.*

3. RESPECT FOR CONTEXT *Consumers have a right to expect companies will collect, use, & disclose personal data in ways that are consistent with the context in which consumers provide the data.*

4. SECURITY *Consumers have a right to secure & responsible handling of personal data.*

5. ACCESS & ACCURACY *Consumers have a right to access & correct personal data in usable formats.*

6. FOCUSED COLLECTION *Consumers have a right to reasonable limits on personal data companies collect & retain. Companies should securely dispose of or de-identify personal data once they no longer need it, unless they have a legal obligation to do otherwise.*

7. ACCOUNTABILITY *Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to these principles.*

Federal Code:
HIPAA Minimum Necessary Standard

- The minimum necessary standard, a key protection of the HIPAA Privacy Rule, is derived from confidentiality codes and practices in common use today. It is based on sound current practice that protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function.

[45 CFR 164.502(b), 164.514(d)]

State Farm's Privacy Principles

- We do not sell customer information.
- We do not allow those who are doing business on our behalf to use our customer information for their own marketing purposes. We contractually require any person or organization providing products or services on our behalf to protect State Farm customer information.
- We do not share customer medical information within the State Farm family of companies unless:
  - you expressly authorize it; or
  - it is permitted or required by law; or
  - your insurance policy contract with us permits us to do so.
- We may share customer information and permit others to use that information if you give us your consent, it is necessary to complete a transaction you request, or it is otherwise permitted by law.
- We handle information about former and prospective customers the same as existing customers.

ACLI
Financial Security for Life

December 2, 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 for the continued opportunity to comment during your ongoing review of past and current consumer privacy frameworks. We appreciate the meaningful and deliberative work that has gone into the NAIC's development of the Privacy Protections Working Group's Privacy Policy Statement and Final Exposure Draft of the Report on Consumer Data Privacy Protections. ACLI appreciates this opportunity to share our member's views on various elements of the final exposure draft.

ACLI is largely supportive of the themes conveyed in the feedback provided by the Joint Trades group. Additionally, there are two topics our members felt warranted a supplemental ACLI response. Those are the rushed process over the final months of the exposure review, as well as the unclear intent of the Appendix section.

Given that the final comment period overlapped with the Thanksgiving Holiday, ACLI requested a brief extension of the comment deadline, which would have allowed us to provide more robust and meaningful feedback to the Working Group. While we appreciate the offer from staff to submit comments in an informal, bullet-point format in lieu of a brief extension of the comment period, we did not feel that format would allow us to thoughtfully and fully communicate our feedback to the Working Group. We believe that ACLI and the Working Group share the same overarching goal as the Working Group- to ensure that this important work is done correctly, thoughtfully, and promptly. We have demonstrated through our constructive engagement throughout this multi-year process that we desire a timely, judicious, and equitable outcome to the efforts of the Privacy Protections Working Group. We prioritize a thorough commitment to "get it right" over the adherence to potentially arbitrary deadlines that may cut against the development of a well-thought-out deliverable.

Still, recognizing the need to provide input on the Working Group's timeline, we are submitting the following comments, along with a detailed, redline version of the exposure draft, that reflects the limited but meaningful feedback we were able to collect from members during the limited exposure period.

1. The Project's Final Push Has Generated Process and Quality Concerns

ACLI recognizes and commends the NAIC Privacy Protections Working Group for their multi-year effort to research potential gaps in consumer data privacy protections due to changes in technology. We acknowledge that there may be gaps in the existing laws that need to be further discussed. We also truly appreciate the significant, deliberate, and thoughtful effort you have made to coordinate with the entire regulatory community, industry, and consumer stakeholders on this complicated issue. However, we question whether the final exposure draft adequately reflects the state of thought of the Working Group members and interested parties because of the rush to be finished in time for presentation at the Fall NAIC meeting. It was evident throughout the biweekly meetings held this fall that there is a vast gulf in understanding between the Consumer Representatives, Industry stakeholders, and Regulators on key issues. These include foundational issues as basic as definitions and scope. Without a clear and common understanding of how key terms were being defined and clarity regarding the goal of the Working Group, it was difficult to offer substantive feedback during the Fall review push.

The development process in Fall 2021 raised some concerns with our members, who were troubled by the cancellation of a crucial meeting as well as the late-stage introduction of a new "consumer right" (data ownership) that had not been publicly discussed by the Privacy Protections Working Group. As we noted above, stakeholders had just two weeks to provide "limited comments" on a final exposure draft that included many substantive revisions from the previous version. The shortened period seems at odds with the typical NAIC exposure period of items containing substantially revised or new issues that haven't been previously exposed for comment.

We understand that consistent stakeholder engagement can feel laborious, in part because it requires Working Groups and Committees to give stakeholders sufficient time to share information, collect feedback, and compile it to share with regulators. Unfortunately, the latest exposure period has not allowed for a thoughtful and meaningful review process merited by this consequential topic.

ACLI serves as a voice of our membership to the NAIC, and we rely heavily on receiving substantive, thoughtful feedback at every stage of the process. It is critical that all stakeholders be given voice by having the necessary time to share information, collect feedback, and compile it to share with the Working Group. The compressed timeline has not allowed for a thoughtful and meaningful review process that a topic this important to consumers and industry alike merits.

Substantively, the final exposure draft includes relatively broad, vague language, some of which may conflict with existing protections in the insurance privacy Models, FCRA, and other privacy laws. This could have the unintended consequence of diminishing the consumer protections that we all agree are necessary. The final exposure draft also contains confusing and, in some areas, inaccurate or outdated material.

The Working Group has acknowledged some of these substantive issues and certainly the tight time frames. Despite this, requests for additional time, even a twenty-four-hour extension to compile received feedback, were denied. Given this rush, we wonder whether there is sufficient time for the Working Group to fully consider and incorporate feedback from all stakeholders prior to the Fall National Meeting.

With more deliberate work, and some additional time, this exposure draft could more solidly reflect the state of the laws/models today and more clearly indicate the open items for future consideration. It could also better reflect the hard work of the Regulators, Industry stakeholders, Consumer advocates, and those involved in this process over the last several years and do more to effectively address the concerns that industry and consumers have in good faith been trying to explore in this group since the beginning.

2. Unclear Intent of the Appendix

As noted in our attached redlined version, the Appendix as written appears to be an aspirational mission statement of what the situation "should be" in relation to consumer data privacy protections. Based on the discussions of the Working Group, as well as the last paragraph of Section VII in the final exposure, the actual purpose of the Appendix appears to serve as an outline for future discussion. These two purposes appear to be in conflict. We recognize that is not the intention of the Working Group and see that as another reason for the need for further conversation. Noting that, we offer the following recommendations for the Working Group's consideration.

- Our redline offers several material corrections and recommended changes to the Appendix.

- This intent of the Working Group could be easily achieved with some simple adjustments to the language of the Appendix. Rather than defining the Appendix as a "Policy Statement," and including words like "should" which may imply that state regulators have determined the content as a matter of policy, we believe clearly and conspicuously framing the Appendix as a roadmap for future discussion would resolve this issue. This would also align with the intent of the Working Group Chair, as expressed during the November 22 meeting.

- The Appendix could be condensed into a few key discussion questions for future inquiry and included within the recommendation section of the final draft exposure. This would more clearly highlight that, as part of their recommendations, the Working Group identified these key issues as being ripe for further discussion. Several interested parties noted on the November 22 call that adjusting the Appendix in this way would alleviate many of their concerns. ACLI agrees with this sentiment.

Conclusion

We appreciate the Working Group's efforts to address this complex topic. We share the goal of ensuring the important work of this group is successful and the final end-product reflects the hard work of the Working Group as well as the input that has occurred over the last several years. We look forward to continuing to work with the NAIC on these important issues.

Sincerely,

Kristin Abbott
Counsel

Shelby Schoensee
Associate Counsel

Privacy Protections (D) Working Group Report on Consumer Data Privacy Protections

Exposure Draft

November 18, 2021

Table of Contents

I. Introduction

The Privacy Protections (D) Working Group was appointed in 2019 to review state insurance privacy protections regarding the collection, use, and disclosure of information gathered in connection with insurance transactions and make recommended changes, as needed, to NAIC models addressing privacy protection. This includes an insurer's use of data collected from a consumer and data supplied to an insurer by a third-party vendor. Rather than focusing on revisions to NAIC models, the main deliverables for 2021 were to set forth a policy statement on the minimum consumer privacy protections that are appropriate for the business of insurance, after taking into consideration the consumer privacy protections that already exist under applicable state and federal laws.

The Working Group discussed how best to balance the rights of insurers to use data for legitimate business purposes with consumers' rights to control what data is used and how it is used. The following privacy protections for consumers were discussed: (1) the right to opt out of data sharing, (2) the right to limit data sharing unless the consumer opts in, (3) the right to correct information, (4) the right to delete information, (5) the right of data portability, (6) the right to restrict the use of data, and (7) ~~the right of data ownership~~, ~~(8)~~ the right of notice~~,~~ ~~and (9) the right of nondiscrimination / non-retaliation~~.

The Working Group received comments from the ACLI, AHIP, APCIA, BCBSA, the Coalition of Health Insurers, NAMIC, MLPA, and NAIC consumer representatives Birny Birnbaum, Brenda Cude, Karrol Kitt, and Harry Ting.

II. Overview of Issue

Consumer awareness and regulatory concerns about the use of consumer data by a variety of commercial, financial, and technology companies are increasing. This has led to adoption of the ~~General Data Protection Regulation (GDPR) in the E.U. and the~~ California Consumer Privacy Act (CCPA) and other state data privacy protection laws in the U.S. Though data privacy concerns extend beyond the insurance sector, the increasing use of data and the passage of these new laws is causing the ~~insurance industry~~business community and consumer groups alike to pressure Congress to enact federal privacy legislation

Commented [ACLI1]: The GDPR was intended to replace the existing 1995 Data Protection Directive (95/46/EC) and provide for greater uniformity between EU Member State adoption of data protection standards. while strengthening consumer online privacy rights and boost Europe's digital economy.

While federal legislative efforts are currently stalled due to other legislative priorities and differing perspectives from consumers and industry on the best path forward, it is likely that Congress will begin focusing on the issue again soon. The current pause provides state insurance regulators an opportunity to update state privacy protections consistent with the current insurance business environment and potentially forestall or mitigate the impacts of any preemptive federal legislation. State policymakers have also responded to the privacy debate with varying legislative proposals to provide consumers with greater transparency and control over the use of personal information, with California, Virginia, and Colorado being leading examples. These comprehensive state data privacy laws each have either entity-level or data-level exemptions for entities subject to or information collected pursuant to the federal Gramm-Leach-Bliley Act (GLBA) and/or the privacy regulations adopted under the Health Insurance Portability and Accountability Act (HIPAA).

III. Summary of Consumer Privacy Protections Provided by NAIC Model Laws

The NAIC has three model laws governing data privacy: *Health Information Privacy Model Act* (Model #55); *NAIC Insurance Information and Privacy Protection Model Act* (#670) and *Privacy of Consumer Financial and Health Information Regulation* (#672), each of which is based upon or influenced by federal privacy laws. The NAIC's Model #670 contains many of the consumer rights found in these comprehensive state laws, which can be traced back to the Fair Credit Reporting Act (FCRA). And Model #672 is based, in large part, on GLBA and the HIPAA regulations. Generally, insurers and other entities licensed by state departments of insurance ~~are carved out~~have certain exemptions from ~~of~~ more comprehensive state laws of general applicability. Because of this, insurance regulators must be aware

when new protections are added to laws applicable to other businesses, especially when they address new technologies and ways consumer information is collected and shared, so that comparable protection can be added, as necessary, to the laws governing the insurance industry. Of note, GLBA and HIPAA each set a federal floor for the entities within their scope, from which states can build upon. This is what the NAIC did in drafting the *Health Information Privacy Model Act* (Model #55) and the *Privacy of Consumer Financial and Health Information Regulation* (#672). GLBA applies to the entire insurance industry and HIPAA applies primarily to the health insurance sector and those which collect or use Protected Health Information.

A. NAIC Insurance Information and Privacy Protection Model Act (Model #670)

The NAIC adopted the *NAIC Insurance Information and Privacy Protection Model Act* (#670) in 1980 following federal enactment of the Fair Credit Reporting Act in 1970 and the Federal Privacy Act in 1974. This model act establishes standards for the collection, use and disclosure of information gathered in connection with insurance transactions by insurance companies, insurance producers and insurance support organizations.

A key aspect of this model is that it establishes a regulatory framework for consumers to (1) ascertain what information is being or has been collected about them in connection with insurance transactions; (2) obtain access to such information for the purpose of verifying or disputing its accuracy; (3) limit the disclosure of information collected in connection with insurance transactions; and (4) obtain the reasons for any adverse underwriting decision.

This regulatory framework is facilitated through a requirement that insurers or agents provide a written notice to all applicants and policyholders regarding the insurer's information practices. The notice must address the following: (1) whether personal information may be collected from persons other than the individual or individuals seeking insurance coverage; (2) the types of personal information that may be collected, the types of sources and investigative techniques that may be used to collect such information; (3) the types of disclosures allowed under the law; (4) a description of the rights established under the law; and (5) notice that information obtained from a report prepared by an insurance support organization may be retained by the insurance support organization and disclosed to other persons.

Of note, the model prohibits disclosure of any personal information about an individual collected or received in connection with an insurance transaction without the individual's written authorization, subject to limited exceptions. However, some categories of information may be disclosed for marketing purposes if the consumer "has been given an opportunity to indicate that he or she does not want personal information disclosed for marketing purposes and has given no indication that he or she does not want the information disclosed,". It also provides consumers with the right to request that an insurer provide access to recorded personal information, disclose the identity of the third parties to whom the insurance company disclosed information (if recorded); disclose the source of collected information (if available); and provide procedures by which the consumer may request correction, amendment, or deletion of recorded personal information.

Seventeen states have adopted Model #670: AZ, CA, CT, GA, HI, IL, KS, MA, ME, MN, MT, NV, NJ, NC, OH, OR, and VA.

B. NAIC Health Information Privacy Model Act (Model #55)

The NAIC adopted the *Health Information Privacy Model Act* (Model #55) following federal adoption of the privacy regulations authorized by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

This model sets standards to protect health information from unauthorized collection, use and disclosure by requiring insurance companies to establish procedures for the treatment of all health information by all insurance carriers. The

drafters of Model #55 believed it was important that the same rules apply to all lines of insurance, since health insurance carriers are not the only ones that use health information to transact their business. For example, health information is necessary for life insurance underwriting, and often essential to property and casualty insurers in settling workers' compensation claims and personal injury liability claims. Reinsurers also use protected health information to write reinsurance.

The model requires carriers to develop and implement written policies, standards, and procedures for the management of health information, including to guard against the unauthorized collection, use or disclosure of protected health information. It provides consumers with the right to access their protected health information and amend any inaccuracies. The model also requires insurers to obtain written authorization ("opt-in") before collecting, using, or disclosing protected health information, except when performing limited activities.

Many of the provisions found in Model #55 were later incorporated into the *Privacy of Consumer Financial and Health Information Regulation* (Model #672).

The following 13 jurisdictions have adopted legislation related to Model #55: CA, CO, DE, KY, LA, ME, MO, ND, RI, SD, TX.

Commented [ACLI2]: Listed are 11 jurisdictions, not 13.

C. NAIC Privacy of Consumer Financial and Health Information Regulation (Model #672)

The NAIC adopted the *Privacy of Consumer Financial and Health Information Model Regulation (Model #672)* in 2000. The model regulation was drafted to implement the requirements set forth in Title V of GLBA. GLBA imposed privacy and security standards on financial institutions, defined to include insurers and other insurance licensees, and directed state insurance commissioners to adopt certain data privacy and data security regulations. The provisions governing protection of financial information are based on privacy regulations promulgated by federal banking agencies. The model also contains provisions governing protection of health information that were taken directly from Model #55 and from the HIPAA Privacy Rule promulgated by the U.S. Department of Health and Human Services (HHS).

The model regulation provides protection for non-public financial and personal health information about consumers held by insurance companies, agents, and other entities engaged in insurance activities. In general, the model regulation requires insurers to: (1) notify consumers about their privacy policies; (2) give consumers the opportunity to ~~prohibit~~ opt out of the sharing of their ~~protected~~ non-public financial information with non-affiliated third parties; and (3) ~~obtain~~ affirmative consent from consumers before sharing ~~protected~~ non-public personal health information with any other parties, affiliates, and non-affiliates subject to certain exceptions, including when necessary to process customer transactions, for purposes required or permissible by law, and when service providers must perform the services.

Commented [ACLI3]: The 672 model recognizes that sharing health information for the business purposes of the disclosing company enables more efficient and effective processes. This benefits both industry and consumers. Moreover, consumers are protected effectively through the complementary provisions requiring that there be contractual assurances limiting use of the data to the approved purposes. This approach is generally consistent with CCPA/CPRA and HIPAA's business associate structure.

The key difference between the treatment of financial information and health information is that insurers must give consumers the right to "opt out" of the disclosure or sharing of their financial information but insurers must obtain explicit authorization from the consumer ("opt-in") before sharing health information for purposes not within an exemption. Every jurisdiction has a version of this model regulation, although nineteen jurisdictions have only adopted the provisions regarding financial information and not the provisions regarding health information. Some jurisdictions that have adopted Model # 670 have adopted additional provisions from Model # 672 by bulletin rather than regulation.

IV. Summary of Health Insurance Portability and Accountability Act (HIPAA)

In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA), which, among other things, authorized the U.S. Department of Health and Human Services (HHS) to promulgate regulations governing consumer privacy protections. The HIPAA Privacy Rule was finalized in 2000. The rule applies to health plans and health care providers, restricting the permitted uses and disclosure of protected health information. HIPAA preempts state law only to the extent that a covered entity or business associate would find it impossible to comply with both the state and federal requirements.

HIPAA provides individuals the right to access and amend their protected health information, the right to request the restriction of uses and disclosures of protected health information, and the right to receive an accounting of disclosures made to other entities.

A covered entity must obtain the individual's written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care operations or otherwise permitted or required by the law. A covered entity is also required to provide notice of its privacy practices.

V. Summary of General Data Protection Regulation (GDPR)

The GDPR became effective in May 2018 and applies to U.S. companies if they (i) "target" individuals in the EU by offering them products or services; or (ii) "monitor" their behavior, as far as that behavior takes place in the EU. ~~collect data from citizens of the E.U. over the internet~~. It requires any organization processing personal data to have a valid legal basis for that personal data processing activity. The GDPR provides six legal bases for processing: Consent; Performance of a Contract; Legitimate Interest; Vital Interest; Legal Requirement; or Public Interest, ~~companies (data "controllers") to obtain explicit consent from consumers to collect their data ("opt in")~~ with an explanation of how the data will be used. It also contains standards for safeguarding the data collected. Under the GDPR, a consumer has the following rights: (1) to receive information about the processing of personal data; (2) to obtain access to the personal data; (3) to request that incorrect, inaccurate or incomplete personal data be corrected; (4) to request that personal data be erased when it is no longer needed or if processing it is unlawful; (5) to object to the processing of personal data ~~for marketing purposes or on grounds relating to a consumer's particular situation~~; (6) to request the restriction of the processing of personal data in specific cases; (7) to receive personal data in a machine-readable format and the ability to ~~send~~ transmit it to another controller if technically feasible ("data portability"); and (8) to request that decisions based solely on automated processing concerning the consumer or significantly affecting the consumer and based on consumer's personal data, are made by human beings~~.~~ or to challenge a decision.

Commented [ACLI4]: The GDPR does not, necessarily, apply to a company simply because it collects data from citizens of the EU over the internet. More is required. Specifically, the company must actively market its products and services to those in the EU. It's a factual determination. For example, routinely shipping goods to the EU, utilizing the French language on the website (in addition to English) and setting the website up to accept euros would likely result in the GDPR applying to a given company.

VI. Summary of Recently Adopted Consumer Privacy Protection Laws

Commented [ACLI5]: In terms of describing the various rights contained within the state privacy laws noted (CA, CO, and VA), such descriptions should be prefaced with "subject to certain limitations."

A. California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)

In 2018, California became the first U.S. state to adopt a comprehensive privacy law applicable beyond the insurance industry, imposing broad obligations on businesses to provide consumers with transparency and control of their personal data. The California Consumer Privacy Act (CCPA) became effective in 2020. Since it was adopted, it was amended by the California Privacy Rights Act (CPRA), which becomes effective Jan. 1, 2023. Additionally, the California Attorney General promulgated implementing regulations in 2020.

Commented [ACLI6]: While there are some differences between CCPA and the 670 model, the core rights to access, deletion, and opt-out are in both. In fact, the 670 model incorporates a right to request correction which goes beyond CCPA.

Scope

The CCPA, as amended by the CPRA (California law) applies to companies doing business in California that collect or process consumers' personal information and meet one of the following thresholds: (1) has annual gross revenue in excess of $25,000,000 in the preceding calendar year; (2) annually buys, sells, or shares the personal information of 100,000 or more consumers or households; or (3) derives 50% or more of its annual revenue from selling or sharing consumers' personal information.

Exemptions

The law does not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (GLBA), and its implementing regulations. It also does not apply to protected health information that is governed by the privacy, security, and breach notification rules issued by ~~the U.S. Department of Health and Human Services (~~HHS~~)~~. Furthermore, this law contains an entity-level exemption for HIPAA-covered entities or business associates governed by the privacy, security, and breach notification rules issued by HHS.

Consumer Rights

California law provides consumers with the following rights : (1) to request deletion of any personal information;[1] (2) to correct inaccurate personal information, taking into account the nature of the personal information and the purposes of the processing of the information; (3) to know about and access the personal information being collected by requesting that the business disclose: the categories and specific pieces of personal information collected, the categories of sources the information was collected from, the business purpose for collecting the information, the categories of third parties with whom the information is shared, and the specific pieces of personal information that was shared; (4) to request the personal information provided by the consumer in a format that is easily understandable, and to the extent technically feasible, in a structured, commonly used, machine-readable format that may also be transmitted to another entity at the consumer's request without hindrance; (5) to know what personal information is sold or shared and to whom; (6) to opt out of the sale ~~or sharing~~ of personal information; (7) to limit the use and disclosure of sensitive personal information aside from the enumerated purposes which are always allowed; and (7) to not be retaliated against for requesting to opt out or exercise other rights under the law.

Business Obligations

The law imposes the following obligations on all covered businesses: (1) prohibits retaining a consumer's personal information for longer than reasonably necessary for the disclosed purpose; (2) requires implementing reasonable security procedures and practices; (3) requires notice of the following: collection of personal information, including sensitive personal information, retention of information, right to opt out of sale and sharing, and financial incentives; (4) prohibits using sensitive personal information outside of enumerated purposes when a consumer has requested not to use or disclose such data.

Enforcement

The CPRA amends the CCPA by placing administrative enforcement authority with the California Privacy Protection Agency, a new state agency created by the CPRA. Under the CPRA, the attorney general retains authority for seeking injunctions and civil penalties. Additionally, if personal information is breached, the consumer can pursue a private civil action against the company.

B. Colorado Privacy Act (CPA)

Scope

The Colorado Privacy Act (CPA) takes effect on July 1, 2023. It applies to entities that conduct business in Colorado or produce or deliver commercial products or services intentionally targeted to residents of Colorado and satisfy one of the following thresholds: (1) controls or processes the personal data of 100,000 or more consumers in a year; or (2)

[1] And even when information is "deleted," the CCPA right to deletion allows the business to "maintain a confidential record of deletion requests solely for the purpose of preventing the personal information of a consumer who has submitted a deletion request from being sold, for compliance with laws or for other purposes."

derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of 25,000 or more consumers. The law defines "controllers" as those that "determine the purposes for and means of processing personal data" and defines "processors" as those that "process data on behalf of a controller."

Exemptions

The law contains data-based exemptions (rather than entity-level exemptions) for protected health information collected, processed, or stored by HIPAA-covered entities and their business associates, and information and documents created by a HIPAA-covered entity for purposes of complying with HIPAA and its implementing regulations. The law also exempts personal information that is maintained by a covered entity or business associate in the same manner as PHI. Additionally, the law specifically exempts financial institutions and personal data subject to the federal Gramm-Leach-Bliley Act (GLBA) ~~contains an exemption for any personal data collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act (GLBA)~~, and its implementing regulations, if such collection, processing, sale, or disclosure is in compliance with that law.

Commented [ACLI7]: The exemptions include: (h) INFORMATION MAINTAINED IN THE SAME MANNER AS INFORMATION UNDER SUBSECTIONS (2)(a) TO (2)(g) OF THIS SECTION BY: (I) A COVERED ENTITY OR BUSINESS ASSOCIATE

Commented [ACLI8]: CPA § 6-1-1304(2)(q)

Consumer Rights

The CPA provides consumers with the following rights: (1) to opt out of targeted advertising, sale of personal data, and profiling; (2) to confirm whether a controller is processing the consumer's personal data and the right to access such data; (3) to correct inaccuracies in personal data; (4) to delete personal data; and (5) to obtain the personal data in a portable and readily usable format that allows the consumer to transmit the data to another entity.

Business Obligations

The CPA imposes affirmative obligations on controllers, including the following: (1) provide consumers with an accessible, clear, and meaningful privacy notice; (2) specify the express purposes for which personal data are collected and processed; (3) collection of personal data must be adequate, relevant and limited to what is reasonably necessary in relation to the specified purposes; (4) not process personal data for purposes that are not reasonably necessary to or compatible with the specified purposes, without obtaining consent from the consumer; (5) take reasonable measures to secure personal data; (6) not process personal data in violation of any law that prohibits unlawful discrimination; and (7) not process a consumer's sensitive data without first obtaining the consumer's consent. Additionally, controllers are required to enter into contracts with data processors, referencing the responsibilities under the CPA and controllers must conduct a data protection assessment prior to any processing activities that have a heightened risk of harm to consumers.

Enforcement

The CPA does not contain a private right of action but provides the state attorney general and district attorneys authority to take action against entities for violations.

C. Virginia Consumer Data Protection Act (CDPA)

Scope

The Virginia Consumer Data Protection Act (CDPA) becomes effective Jan. 1, 2023. It applies to entities that conduct business in Virginia or produce products or services targeted to Virginia residents when they control or process personal data of at least 100,000 consumers or control or process personal data of at least 25,000 consumers and also derive over 50% of gross revenue from the sale of personal data.

Exemptions

The law contains entity-level exemptions for those subject to GLBA and HIPAA. It specifically exempts financial institutions and data subject to GLBA, and covered entities or business associates governed by the privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services. It also exempts protected health information under HIPAA.

Consumer Rights

The CDPA provides consumers with the following rights: (1) to confirm whether or not a controller is processing the consumer's personal data and if so, to provide the right to access such personal data; (2) to correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of processing of the consumer's personal data; (3) to delete personal data provided by or obtained about the consumer; (4) to obtain a copy of the consumer's personal data in a portable and readily usable format that allows the consumer to transmit the data to another controller; and (5) to opt out of the processing of the personal data for purposes of targeted advertising, sale of personal data, and profiling.

Business Obligations

Under the law, controllers have the responsibility to do the following: (1) limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed; (2) not process personal data without consumer consent for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such personal data is processed; (3) establish, implement, and maintain reasonable data security practices to protect personal data; (4) not process personal data in violation of any laws that prohibit unlawful discrimination against consumers and not discriminate against consumers exercising their rights under this law; and (5) not process sensitive data concerning a consumer without obtaining the consumer's consent. In addition, controllers must provide consumers with a reasonably accessible, clear, and meaningful privacy notice. Processing activities undertaken by a processor on behalf of a controller must be governed by a data processing agreement. Controllers also must conduct data protection assessments that evaluate the risks associated with processing activities.

Enforcement

Similar to the Colorado law, the law does not contain a private right of action but provides the state attorney general authority to pursue action against entities for violations.

VII. Summary of Working Group Discussions of Selected Key Points

The working group began discussions Dec. 8, 2019, during the Fall National Meeting with the following minimum consumer privacy protections being considered as appropriate for the business of insurance. These rights were based on the Working Group's proposed 2020 charges and are included in the Working Group's initial 2019 Work Plan:

1. the right to receive notice of an insurer's privacy policies and practices;
2. the right to limit an insurer's disclosure of personal data;
3. the right to have access to personal data used by an insurer;
4. the right to request the correction or amendment of personal data used by an insurer;
5. the right of data ownership; and
6. the right of data portability.

The Work Plan also said that the Working Group discussions would focus on data privacy (rather than data security) and identify areas within NAIC models and state requirement where consumer data privacy protections might need to

be enhanced due to changes in technology. In her Dec. 8 presentation, Jennifer McAdam (NAIC) outlined existing privacy provisions in NAIC models and state insurance laws. She said the difference between data privacy and data security is that data privacy is about how data is being collected and used by businesses; while data security is about how data that a business has already collected and has in its possession) is stored and protected from unauthorized access. She said the two are often conflated and there are some laws that address both – like GDPR, for example. Furthermore, as many comments have noted, the two issues overlap because a breach of security often results in a loss of privacy. Ms. McAdam said the CCPA is an example of a data privacy law that governs how businesses collect and use consumer data; the rights consumers have to know how that data is being used; the rights consumers have to challenge the accuracy of the data; and how it is being used. Data privacy laws are focused on legal protections for data and consumer rights: In comparison, data security laws, such as the NAIC's Insurance Data Security Model Law (#668), require operational and technological protections sufficient to ensure that the legal protections are meaningful. Ms. McAdam explained that Model #668 governs how businesses protect the data once it has been collected as well as what businesses need to do if those protections fail as the result of a data breach or other cybersecurity event.

State insurance regulators were concerned about the consumer data that insurers were already presenting in rate filings that had ballooned up to thousands of pages of different data points being gathered by insurers on consumers. They have also seen an increased reliance on third-party risk scores that aggregate consumer information in order to make determinations and conclusions about that information. Regulators noted that insurers have a responsibility to ensure that the third parties used are following state laws and complying with the state's standards for accuracy and fairness. In addition to providing disclosure of the third parties used by insurers when consumers request it, insurers are required to report how the information was gathered; where it was drawn from (e.g., web traffic, geolocation data, social media, etc.); and why the company thinks it needs to use those particular data points as the possibilities available to insurers are endless.

Industry asked the Working Group to consider: 1) Workability by allowing for various exemptions for operational and other reasons that acknowledge vital business purposes for insurers to collect, use, and disclose information. For example, Article IV of the NAIC Model #672 was developed to implement the GLBA, and the exceptions embedded into Section 13 of Model #672 are instructive as to the types of operational functions that need to be preserved and facilitated; 2) Exclusivity by avoiding dual regulation, so insurers are not simultaneously subject to potentially inconsistent or conflicting interpretations by more than one regulator; 3) Clarity by asking that care be taken to consider how best to dovetail with existing models/ laws/regulations; consulting other resources and educating legislators on how privacy bill language impacts the insurance industry, including the legal requirements to retain and use certain data, as well as data mandates; 4) an effective date that allows advance time (like the two to five years that was afforded under the GDPR) for insurers to be ready for implementation, to avoid having piecemeal revisions like the CCPA ~~and the GDPR~~, as well as a roll-out period with different dates for different provisions within that time frame as a more measured approach to undertake such a significant endeavor.

Consumer Representatives asked the Working Group to consider that: 1) Data vendors are scraping personal consumer information from public sources to produce consumer profiles, scores, and other tools for insurers. The data vendor products, while assembled from public information, raise concerns over consumers' digital rights and privacy; 2) Many data vendors and many types of personal consumer information are not subject to FCRA consumer protections. In turn, many of the types of data and algorithms used by insurers are not subject to either FCRA consumer protections (even though they are the functional equivalent of a consumer report) or the NAIC model law/regulation protections; 3) It is unclear whether the NAIC models cover the new types of data being generated by consumers as part of, or related to, insurance transactions. For example, consumers are producing large volumes of data through telematics programs from devices collecting personal consumer data in the vehicle or home or through wearable devices; 4) There are a lots of organizations working on consumer digital rights (such as the Center for Digital Democracy, the

Electronic Privacy Information Center, the Electronic Frontier Foundation, the Public Knowledge-Privacy Rights Clearinghouse, the Public Citizen, the U.S. Public Interest Research Group, and the World Privacy Forum) from whom input and presentations at Working Group meetings should be solicited; and 5) If consumer disclosures are to be used, that the disclosure should be a compliance or enforcement tool that would be created using consumer focus testing and established best practices for the creation of such consumer disclosures.

Commented [ACLI9]: The asks from the consumer reps are not clear. What are "consumer disclosures" and "compliance or enforcement tool", and what are the consumer reps trying to achieve?

The COVID-19 pandemic slowed down the Working Group's discussions in 2020; however, discussions continued through seven virtual meetings and two regulator-only meetings of subject matter experts as areas of concentration were being narrowed leading to the Working Group requesting additional guidance from its parent committee.

In April 2021, the Working Group's discussions were redirected to six consumer data privacy rights or types of consumer data privacy protections based on the specific examples identified in item 1.c. of the NAIC Member Adopted Strategy for Consumer Data Privacy Protections received through its parent Committee, the Market Regulation and Consumer Affairs (D) Committee. The Working Group's task was to comment on the following consumer privacy rights concerning consumers' personal information as a basis for a privacy protection framework for the insurance industry (not just health insurance):

1. Right to opt out of data sharing;
2. Right to limit data sharing unless the consumer opts in;
3. Right to correct information;
4. Right to delete information;
5. Right to data portability;
6. Right to restrict the use of data.

Consequently, the Working Group was also tasked with analyzing or determining how insurers were protecting these rights – either to comply with state or federal statutory or regulatory requirements, or on their own initiative or through the adoption of voluntary standards. In 2021, the Working Group met ten times and the regulator only subject matter experts met nine times.

Prior to the 2021 Summer National Meeting, Working Group discussions focused on discussion of, and input on, the following key points from regulators, industry, and consumers for each of the six consumer privacy data rights noted above: definition; examples; consumer risk/impact; current state and federal laws/rules; insurer/licensee impact; actions necessary/insurer obligations to minimize consumer harm; and recommendations. Suggestions that separate privacy requirements be established for each line of business were discussed, but there was consensus that they did not seem to be feasible, as different consumer data privacy requirements across lines of business would limit both consumer protections and understanding.

It was noted during Working Group discussions that insurers utilize third party vendors as sources of data collection and that such vendors may not be subject to regulation by state insurance departments. Regulators stated that the insurers they regulate bear the responsibility for compliance with state insurance privacy requirements. Insurers felt they could not be held responsible because they did not know how such vendors collected or used consumer data and had no way to control the vendors business activities. Regulators and consumer representatives expressed different opinions indicating that insurers' contracts with such vendors could and should be written to require vendors and insurers maintain compliance with insurance regulations regarding consumer data privacy.

Commented [ACLI10]: This is extremely onerous for the insurance industry to enforce, as this would de facto require the insurance company to be enforcers of insurance privacy regulations across different industries. Perhaps Safe harbor exemptions can be considered (e.g., require the vendor to warrant that it complies with CCPA or other applicable state laws).

During the 2021 Summer National Meeting, NAIC members further recommended that the Working Group's discussion be expanded to include the issue of consumer data ownership.

Working Group discussions revealed that state insurance regulators and consumer representatives believe consumers own the data that is collected and used by the insurance industry to market, sell, and issue insurance policies. It was

felt that the type of data collected (name, age, date of birth, height, weight, income, physical condition, personal habits, etc.) describes who a person is and distinguishes one person from another by its very nature. When a consumer shares their data with an insurance company, it is with the understanding that the consumer is letting the company borrow it for a time to determine what insurance rates and insurance coverage the consumer needs. The consumer is not giving up their data to an insurer so it can be sold or given to other organizations from whom the consumer is not seeking insurance coverage, or any other product. Consumer representatives indicated that this practice had happened when they did an online search for insurance rates on health plans. As a result, the consumer representative received hundreds of cold calls from companies selling products other than insurance. When the consumer representative asked with whom the insurance company shared his data, the company sent him a list of 1,700 companies – none of which sold insurance.

The privacy policy statement in Appendix A is designed to be the foundation for the minimum consumer data privacy protections that are appropriate for the business of insurance to be applied to NAIC model #672 as revisions. It is intended to kick start the next step in creating revisions by defining the parameters of the existing consumer data privacy rights; by suggesting definitions and by showing examples of consumer risks. Further discussion is necessary, however, to clarify consumer data privacy rights that may not be fully protected in federal laws or fully covered under NAIC Model laws, and to decide how to provide appropriate protections.

VIII. Conclusion and Recommendations

Months of detailed discussions with regulator, industry, and consumer stakeholders, and the comments they have submitted, have led the Working Group to determine that the *NAIC Insurance Information and Privacy Protection Model Act (Model #670)* and the *Privacy of Consumer Financial and Health Information Regulation (Model #672)* have in the past provided an effective regulatory framework for consumer privacy protections to oversee and enforce consumer data privacy as required by state and federal statutes and regulation. However, these models were adopted by the NAIC 20 and 40 years ago, respectively; with only 17 jurisdictions adopting Model #670.

In consideration of the many changes that have occurred in recent years, as well as the rate of increase in the use of new technologies (AI, machine learning, accelerated underwriting, rating algorithms, etc.), and big data by insurers, the Working Group recommends that models 670 and 672 be amended to ensure that regulators can continue to provide consumer data privacy protections essential to meet the consumer data privacy challenges presented by the public use of technology and data by insurers in today's business environment.

The Working Group also recommends the NAIC's Market Regulation Handbook be updated, as necessary, to provide guidance to state insurance regulators so they can verify insurers' compliance with the regulatory framework for consumer privacy protections.

Commented [ACLI11]: Suggestion to delete appendix, and, in this space, bullet point key issues identified in the appendix- clearly identifying them as outstanding issues needing further discussion.

Appendix A

National Association of Insurance Commissioners
Policy Statement on Consumer Data Privacy Protections

Because the business operations of insurance companies are dependent upon the collection and use of personal information and data, state insurance regulators have long understood the need to balance an insurance company's need to collect consumer information and data with the consumer's right to limit the collection and use of data.

The NAIC adopted the *Insurance Information and Privacy Protection Model Act* (Model #670) in 1980 to establish standards for the collection, use and disclosure of information gathered in connection with insurance transactions. A key aspect of this model is that it establishes a regulatory framework for consumers to (1) ascertain what information is being or has been collected about them in connection with insurance transactions; (2) obtain access to such information for the purpose of verifying or disputing its accuracy; (3) limit the disclosure of information collected in connection with insurance transactions; and (4) obtain the reasons for any adverse underwriting decision. This regulatory framework is facilitated through a requirement that insurers or agents provide a written notice to all applicants and policyholders regarding the insurer's information practices.

The NAIC adopted the *Privacy of Consumer Financial and Health Information Model Regulation* (Model #672) in 2000. The model regulation was drafted to implement the requirements set forth in Title V of the federal *Gramm-Leach-Bliley Act* (P.L. 106-102) of 1999 (GLBA). GLBA imposed privacy and security standards on financial institutions and directed state insurance commissioners to adopt certain data privacy and data security regulations. The model also contains provisions governing protection of health information that were taken directly from the Health Insurance Portability and Accountability Act Privacy Rule promulgated by HHS. The NAIC model regulation requires insurers to: (1) notify consumers about their privacy policies; (2) give consumers the opportunity to ~~prohibit~~ opt-out of the sharing of their ~~protected~~ non-public financial information with non-affiliated third parties; and (3) obtain affirmative consent from consumers before sharing ~~protected~~ non-public personal health information with any other parties, affiliates, and non-affiliates, subject to certain exceptions, including when necessary to process customer transactions, for purposes required or permissible by law, and when service providers must perform the services. The key difference between the treatment of financial information and health information is that insurers must give consumers the right (with limited exceptions) to "opt out" of the disclosure or sharing of their non-public financial information to third-parties for the third-party's own business use,, but insurers must get explicit authorization ("opt in") before sharing health information absent an applicable exception.

This ~~policy statement~~ Appendix is based on the consumer protections set forth in these two models and serves the purpose of informing licensed insurance entities, consumers, and the other state and federal regulatory agencies on what the NAIC currently supports as the minimum consumer data privacy protections that are appropriate for the business of insurance. The ~~policy statement~~Appendix is not intended to modify any existing NAIC models and does not carry the weight of law or impose any legal obligations in states that have adopted those models. Instead, this Appendix is meant to highlight issues needing further discussion with Regulators, Industry, and Consumer Reps.

The ~~policy statement~~Appendix addresses consumer data privacy protections of (1) transparency; (2) consumer control; (3) consumer access; (4) data accuracy; and (5) data ~~ownership and~~ portability. The ~~policy statement~~Appendix intentionally excludes standards for data security and standards for the investigation and notification to an insurance commissioner of a licensed insurance entity's cybersecurity event, which are the subject of separate model laws and interpretive guidance.

Commented [ACLI12]: In light of the array of deficiencies, we believe this Appendix should be deleted in its entirety. It would be ill-advised to incorporate partially-formed ideas into the paper when there is no need or clear purpose for doing so.

Commented [ACLI13]: Roadmap for Future Discussion?

Commented [ACLI14]: Add a disclaimer that this is intended to highlight issues needing further discussion with Regulators, Industry, and Consumer Reps.

Commented [ACLI15]: Data Ownership has not been openly discussed with industry.

The following definitions are used for the purposes of this ~~policy statement~~Appendix.

A. "Adverse Decision" means declination of insurance coverage, termination of insurance coverage, charging a higher rate for insurance coverage, or denying a claim.

B. "Consumer" means an individual who is seeking to obtain, obtaining, or has ~~have~~ obtained a product or service from an insurer. For example, an individual who has submitted an application for insurance is a consumer of the company to which he or she has applied, as is an individual whose policy with the company has expired.

C. "Customer" means a consumer with whom an insurer has an on-going relationship.

D. "Licensee" means any insurer, producer, or other person licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to a state insurance law.

E. ~~"~~"Personal Information"~~"~~ means any individually identifiable information or data gathered in connection with an insurance transaction from which judgments can be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit, health, or any other personal characteristics. Personal information includes:

1. "Non-Public Personal Information," which means information that a consumer provides to a licensee to obtain an insurance product or service (like income, credit history, name and address); information about a consumer a licensee has as a result of a transaction involving an insurance product or service (like premium payment history, how much a life insurance policy is worth, and the value of personal property insured); and all other information about a consumer that a licensee uses in connection with providing a product or service to a consumer.
2. "Non-public personal health information," which means any information that identifies a consumer in some way, and includes information about a consumer's health, including past and present physical and mental health, details about health care, and payment for health care.

I. Transparency

A licensee should provide a clear and conspicuous notice to consumers that accurately reflects its privacy policies and practices when it first requests personal information about the consumer from the consumer or upon first contact with the consumer if personal information is collected from a third party.

A licensee should also provide a periodic notice of its privacy policies and practices to customers not less than annually during the continuation of the customer relationship or, alternatively, have privacy policy posted on customer facing website.

If a licensee makes an adverse decision based on information/data that was not supplied by the consumer, the licensee should provide the consumer with the specific reasons for the adverse decision.

II. Consumer Control

Licensees should, at a minimum, provide consumers the opportunity to ~~prohibit~~ limit the sharing of their non-public personal information with third parties, except for specific purposes required in connection with the purpose for which the personal information was collected, ~~required~~ or specifically permitted by law. (Opt-Out)

Licensees should obtain affirmative consent from consumers before sharing non-public personal health information with any other entity, including its affiliates and non-affiliates, subject to certain exceptions, including when necessary to process customer transactions, for purposes required or permissible by law, and when service providers must perform the services.. (Opt-In)

Commented [ACLI16]: These definitions should be exactly as they appear in the current NAIC Model 672 and 670

Commented [ACLI17]: The definition of consumer should be tied to one who seeks to obtain or makes an inquiry in regard to a product or service to be used primarily for personal, family or household purposes.

Commented [ACLI18]: Personal information should be tied to a "Consumer" rather than to an insurance transaction to avoid the unintended consequence of narrowing the scope of PI being regulated. Also, shouldn't there be consideration of beneficiaries, insureds, owners, and payers since they may not be the same people and may not fall under the definition of "Consumer" or "Customer" as currently expressed.

Commented [ACLI19]: An annual delivery requirement contradicts the FAST Act amendments to the GLBA.

III. Consumer Access

Any consumer should have the right to submit a request to a licensee to obtain access to his/her personal information within licensee's possession or control.~~access to his/her personal information used by the licensee in its operations~~. Upon request, the licensee should within 30 business days provide a copy of the consumer's personal information, an explanation on how the personal information was used (i.e., rating, underwriting, claims), and provide the categories of sources of the personal information. If personal information is in coded form, the licensee should provide an accurate ~~translation~~ summary in plain language.

IV. Data Accuracy

Within 30 business days after receiving a request from a consumer to correct, amend, or delete personal information used by the licensee in its operations, the licensee should either make the requested correction, amendment, or deletion or notify the consumer of its refusal to do so, the reasons for the refusal, in the case of a refusal to make a correction or amendment, and the consumer's right to file a statement of dispute setting forth what the consumer thinks is the correct information and the reasons for disagreeing with the licensee.

If the licensee corrects, amends, or deletes personal information, the licensee should notify any person or entity that the licensee knows has received the prior personal information within the last 7 years. If the licensee does not correct, amend, or delete the disputed personal information, the licensee should notify any person or entity that has received the prior personal information within the last 7 years of the consumer's statement of dispute.

V. Data ~~Ownership and~~ Portability

A customer should have the right to request a copy of his/her personal information that he/she has provided to the licensee for use in the licensee's operations. A licensee should provide a customer a copy of his/her personal information within 30 business days of the request. Examples of this type of personal information include telematics data and "Internet of Things" ("IoT") data.

Commented [ACLI20]: Consumer access should be qualified to reflect anti-fraud, identity theft and security considerations. Verification of the consumer and the request are critical components. Also, exceptions to provision of certain information should be recognized.

Commented [ACLI21]: It would be exceptionally burdensome to enumerate "the source of the personal information." This is not required by other laws. For example, CPRA requires disclosure of the categories of sources from which the consumer's personal information was collected. This approach strikes the appropriate balance to ensure meaningful disclosure without adding significant cost to industry that will have little consumer benefit.

Commented [ACLI22]: If an insurance company had to pay for the information, charging the fees the insurance company had to incur, may be reasonable, especially when the insurance company did not secure business from the consumer.

Commented [ACLI23]: This should allow for a description rather than a literal translation or replication.

Commented [ACLI24]: This lookback should remain two years or seven years depending on whether it was an insurance support institution, as per the #670 Model

Commented [ACLI25]: Notifying all recipients within the last seven years will present significant burden to industry with little consumer benefit and absurd results. For example, if a vendor relationship was entered into six years ago, but ended four years ago and data has been archived or deleted, the obligation to notify would still apply.

Commented [ACLI26]: This provision should be reviewed in its entirety because it relates to access, as opposed to ownership or portability.

Commented [ACLI27]: This is too prescriptive and it is unreasonable to think that a consumer would have the capacity to read or interpret all of the IoT data, if it was even technically feasible for an insurer to grant access to such raw data.

Commented [ACLI28]: This should be excluded to the extent it is not personal data. For example, a driver for a delivery service or trucking company may have devices that capture telematics, but the vehicle may be shared and the data would be specific to the vehicle not the individual.

December 2, 2021

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

By Email to Lois Alexander at LAlexander@NAIC.org

Re: Final Exposure Draft Report to D Committee, 11.18.21

Dear Ms. Amann:

On behalf of the members of America's Health Insurance Plans (AHIP), I appreciate the opportunity to provide comments on the Draft Report released on November 18, 2021, and discussed during the Working Group's meeting on Monday, November 22, 2021. It is hoped that submitting both these written comments and a redline of the Draft Report will be helpful to you and the Working Group members.

This working group and Industry have been working on this effort for approximately two years. Throughout that process, it has been difficult to discern the direction or preferences of the working group on any of the privacy protections discussed. It is not reasonable to assume that now, this Final Exposure Draft, with a comment period of only 8 business days, can be adequately reviewed by members of the various trade groups and comments distilled down to only "minor edits".

We will therefore offer three alternative options as our recommendations. Options 1 and 2 are the most simple and brief. Option 3 is a more traditional approach, using more specific comments and a redline of the Final Exposure Draft.

- **Option 1.** For this approach, we'd recommend reducing the Final Exposure Report so that it consists of only the three paragraphs which now make up **VIII. Conclusions and Recommendations**.

- **Option 2.** A variation of this approach would be to delete the Appendix, so that the final document consists of the first twelve (12) pages alone.

The rationale for both Option 1 and Option 2 is that the material in the first 12 pages is largely summary and contains various errors and internal conflicting positions. Additionally, the

Appendix is duplicative of material in the first twelve pages, and in some cases, it too is confusing and conflicting. Option 1 reduces the Final Report to a more accurate, easily understandable document, and Option 2 would add to the Report the background and explanations which are found in the first 12 pages.

- **Option 3**. This is the more traditional approach in which we've attempted to quickly pick out the more obvious concerns, confusing language, and inaccurate statements. We have set those issues out in the attached redline of the Final Exposure Draft and the following comments.

A. Most of the changes made in the redline are self-explanatory, but the language in **Introduction** needs some added clarity. It seems to indicate the purpose of the Report is:

> "…to set forth a policy statement on the minimum consumer privacy protections that are appropriate for the business of insurance, after taking into consideration the consumer privacy protections that already exist under applicable state and federal laws." (Emphasis added)

This seems to conflict with similar language about the Report's purpose in Appendix A, page 13:

> "This policy statement is based on the consumer protections set forth in these two models and serves the purpose of informing licensed insurance entities, consumers, and the other state and federal regulatory agencies on what the NAIC currently supports as the minimum consumer data privacy protections that are appropriate for the business of insurance." (Emphasis added)

This first paragraph seems to say the document is based on unnamed federal and state laws, while the second is based on the two models.

B. Another concern arose as we read the Final Exposure Draft and learned there had been 11 regulator-only meetings on this issue, apparently with some unnamed subject matter experts. We'd like to ask who these experts were, and when these meetings occurred. Also, will there be additional regulator-only meetings on this issue, and if so, will Industry be advised of them in advance? We are not only surprised to learn of these meetings just now, but also disappointed since many of us might have had useful information that could have eased some of the tasks being undertaken.

C. We appreciate your comments during Monday's meeting to the effect that you viewed this document as a "status quo" report of sorts, to outline the currently existing protections supported by the NAIC, and that no decisions had yet been made on how or whether those protections should be modified.

D. We also would repeat some of the suggestions made by interested parties during the meeting, including that this Report should refer to the various "rights" by another term, such as "protections" or "issues". We also suggest that the various definitions and protections cited in

the Report be cross-referenced by section to the Model from which it came, or otherwise identify the source of the language used if not from Model #670 or #672.

E. It was surprising and confusing to learn that the Working Group has decided to recommend that both Models #670 and #672 should be amended, when previous discussions and at least one notice from the Working Group on June 29, 2020 indicated that #672 would be the foundation from which the Working Group would base its work. Additionally, on page 12 of the Final Exposure Draft, two conflicting positions are taken – to work on amendments on both #670 and #672, and to work on amendments to #672 alone. There is no need to include Model #670 in future efforts, as it has not been broadly accepted in the states and part of the effort to develop #672 was to set out the more developed views of regulators at that time.

F. Next, it bears noting that the April 29, 2020 comment letter submitted by the Joint Trades – ACLI, APCIA, AHIP, BCBSA, the Big I, and NAMIC - recommended that the Working Group conduct a two-phase "Gap Analysis." The first phase would be to engage in a public, comprehensive review of the existing federal and state privacy requirements. This was done, in part with the assistance of the trades in presenting a comparison of some of those requirements in the Summer of 2020. The second phase would then be to assemble a list of areas in which regulators believed the existing laws failed to adequately protect consumers. This would set the stage for meaningful fact-based policy discussions by regulators, industry, and consumer representatives which would culminate in a draft of positions on how Model #672 could be amended, or a determination that no such modernization was needed or practical. It is this second phase which has not yet occurred, and if this Working Group is not going to do it, it should be a part of any recommendations made to the Market Regulation and Consumer Affairs (D) Committee.

It must be stated that these comments are only the results of hurried reviews by our members due to the abbreviated comment time. They are not intended to be all-inclusive or complete, but without their implementation, the Final Exposure Draft is not sufficiently accurate or clear to be ready for adoption or delivery to the (D) Committee.

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

Sincerely,

Bob Ridgeway
Bridgeway@ahip.org
501-333-2621

Privacy Protections (D) Working Group Report on Consumer Data Privacy Protections

Exposure Draft

November 18, 2021

Table of Contents

I. Introduction

The Privacy Protections (D) Working Group was appointed in 2019 to review state insurance privacy protections regarding the collection, use, and disclosure of information gathered in connection with insurance transactions and make recommended changes, as needed, to NAIC models addressing privacy protection. This includes an insurer's use of data collected from a consumer and data supplied to an insurer by a third-party vendor. Rather than focusing on revisions to NAIC models, the main deliverables for 2021 were to set forth a policy statement on the minimum consumer privacy protections that are appropriate for the business of insurance, after taking into consideration the consumer privacy protections that already exist under applicable state and federal laws.

The Working Group discussed how best to balance the rights of insurers to use data for legitimate business purposes with consumers' rights to control what data is used and how it is used. The following privacy protections for consumers were discussed: (1) the right to opt out of data sharing, (2) the right to limit data sharing unless the consumer opts in, (3) the right to correct information, (4) the right to delete information, (5) the right of data portability, (6) the right to restrict the use of data, ~~(7) the right of data ownership,~~ and (8) the right of notice~~, and (9) the right of nondiscrimination / non-retaliation~~.

Commented [RB1]: To the extent these were discussed, it was in cursory fashion. Written comments requested and submitted by interested parties were primarily limited to the six "rights" set out in the comment schedule.

The Working Group received comments from the ACLI, AHIP, APCIA, BCBSA, the Coalition of Health Insurers, NAMIC, MLPA, and NAIC consumer representatives Birny Birnbaum, Brenda Cude, Karrol Kitt, and Harry Ting.

II. Overview of Issue

Consumer awareness and regulatory concerns about the use of consumer data by a variety of commercial, financial, and technology companies are increasing. This has led to adoption of the General Data Protection Regulation (GDPR) in the E.U. and the California Consumer Privacy Act (CCPA) and other state data privacy protection laws in the U.S. Though data privacy concerns extend beyond the insurance sector, the increasing use of data and the passage of these new laws is causing the insurance industry and consumer groups alike to pressure Congress to enact federal privacy legislation.

While federal legislative efforts are currently stalled due to other legislative priorities and differing perspectives from consumers and industry on the best path forward, it is likely that Congress will begin focusing on the issue again soon. The current pause provides state insurance regulators an opportunity to update state privacy protections consistent with the current insurance business environment and potentially forestall or mitigate the impacts of any preemptive federal legislation. State policymakers have also responded to the privacy debate with varying legislative proposals to provide consumers with greater transparency and control over the use of personal information, with California, Virginia, and Colorado being leading examples. These comprehensive state data privacy laws each have either entity-level or data-level exemptions for entities subject to or information collected pursuant to the federal Gramm-Leach-Bliley Act (GLBA) and/or the privacy regulations adopted under the Health Insurance Portability and Accountability Act (HIPAA).

Formatted: Underline

Formatted: Underline

Commented [RB2]: Is it appropriate to cite this as a prime motivator for this effort, particularly in view of the last sentence of the paragraph above?

Formatted: Underline

III. Summary of Consumer Privacy Protections Provided by NAIC Model Laws

The NAIC has three model laws governing data privacy: *Health Information Privacy Model Act* (Model #55); *NAIC Insurance Information and Privacy Protection Model Act* (#670) and *Privacy of Consumer Financial and Health Information Regulation* (#672), each of which is based upon or influenced by federal privacy laws. The NAIC's Model #670 contains many of the consumer rights found in these comprehensive state laws, which can be traced back to the Fair Credit Reporting Act (FCRA). And Model #672 is based, in large part, on GLBA and the HIPAA regulations. Generally, insurers and other entities licensed by state departments of insurance are carved out of more comprehensive state laws of general applicability. Because of this, insurance regulators must be aware when new protections are

added to laws applicable to other businesses, especially when they address new technologies and ways consumer information is collected and shared, so that comparable protection can be added, as necessary, to the laws governing the insurance industry. Of note, GLBA and HIPAA each set a federal floor for the entities within their scope, from which states can build upon. This is what the NAIC did in drafting the *Health Information Privacy Model Act* (Model #55) and the *Privacy of Consumer Financial and Health Information Regulation* (#672). GLBA applies to the entire insurance industry while HIPAA applies primarily to the health insurance sector but also impacts other lines to the extent they use Protected Health Information. .

A. NAIC Insurance Information and Privacy Protection Model Act (Model #670)

The NAIC adopted the *NAIC Insurance Information and Privacy Protection Model Act* (#670) in 1980 following federal enactment of the Fair Credit Reporting Act in 1970 and the Federal Privacy Act in 1974. This model act establishes standards for the collection, use, and disclosure of information gathered in connection with insurance transactions by insurance companies, insurance producers, and insurance support organizations.

A key aspect of this model is that it establishes a regulatory framework for consumers to (1) ascertain what information is being or has been collected about them in connection with insurance transactions; (2) obtain access to such information for the purpose of verifying or disputing its accuracy; (3) limit the disclosure of information collected in connection with insurance transactions; and (4) obtain the reasons for any adverse underwriting decision.

This regulatory framework is facilitated through a requirement that insurers or agents provide a written notice to all applicants and policyholders regarding the insurer's information practices. The notice must address the following: (1) whether personal information may be collected from persons other than the individual or individuals seeking insurance coverage; (2) the types of personal information that may be collected, the types of sources and investigative techniques that may be used to collect such information; (3) the types of disclosures allowed under the law; (4) a description of the rights established under the law; and (5) notice that information obtained from a report prepared by an insurance support organization may be retained by the insurance support organization and disclosed to other persons.

Of note, the model prohibits disclosure of any personal information about an individual collected or received in connection with an insurance transaction without the individual's written authorization, subject to limited exceptions. However, some categories of information may be disclosed for marketing purposes if the consumer "has been given an opportunity to indicate that he or she does not want personal information disclosed for marketing purposes and has given no indication that he or she does not want the information disclosed," It also provides consumers with the right to request that an insurer provide access to recorded personal information;, disclose the identity of the third parties to whom the insurance company disclosed information (if recorded); disclose the source of collected information (if available); and provide procedures by which the consumer may request correction, amendment, or deletion of recorded personal information.

Seventeen states have adopted Model #670: AZ, CA, CT, GA, HI, IL, KS, MA, ME, MN, MT, NV, NJ, NC, OH, OR, and VA.

B. NAIC Health Information Privacy Model Act (Model #55)

The NAIC adopted the *Health Information Privacy Model Act* (Model #55) following federal adoption of the privacy regulations authorized by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

This model sets standards to protect health information from unauthorized collection, use and disclosure by requiring insurance companies to establish procedures for the treatment of all health information by all insurance carriers. The

drafters of Model #55 believed it was important that the same rules apply to all lines of insurance, since health insurance carriers are not the only ones that use health information to transact their business. For example, health information is necessary for life insurance underwriting, and often essential to property and casualty insurers in settling workers' compensation claims and personal injury liability claims. Reinsurers also use protected health information to write reinsurance.

The model requires carriers to develop and implement written policies, standards, and procedures for the management of health information, including to guard against the unauthorized collection, use or disclosure of protected health information. It provides consumers with the right to access their protected health information and amend any inaccuracies. The model also requires insurers to obtain written authorization ("opt-in") before collecting, using, or disclosing protected health information, except when performing limited activities.

Many of the provisions found in Model #55 were later incorporated into the *Privacy of Consumer Financial and Health Information Regulation* (Model #672).

The following 13 jurisdictions have adopted legislation related to Model #55: CA, CO, DE, KY, LA, ME, MO, ND, RI, SD, TX.

C. NAIC Privacy of Consumer Financial and Health Information Regulation (Model #672)

The NAIC adopted the *Privacy of Consumer Financial and Health Information Model Regulation (Model #672)* in 2000. The model regulation was drafted to implement the requirements set forth in Title V of GLBA. GLBA imposed privacy and security standards on financial institutions, defined to include insurers and other insurance licensees, and directed state insurance commissioners to adopt certain data privacy and data security regulations. The provisions governing protection of financial information are based on privacy regulations promulgated by federal banking agencies. The model also contains provisions governing protection of health information that were taken directly from Model #55 and from the HIPAA Privacy Rule promulgated by HHS.

The model regulation provides protection for financial and health information about consumers held by insurance companies, agents, and other entities engaged in insurance activities. In general, the model regulation requires insurers to: (1) notify consumers about their privacy policies; (2) give consumers the opportunity to prohibit the sharing of their protected financial information with non-affiliated third parties; and (3) obtain affirmative consent from consumers before sharing protected health information with any other parties, affiliates, and non-affiliates.

The key difference between the treatment of financial information and health information is that insurers must give consumers the right to "opt out" of the disclosure or sharing of their financial information but insurers must obtain explicit authorization from the consumer ("opt-in") before sharing health information. Every jurisdiction has a version of this model regulation, although nineteen jurisdictions have only adopted the provisions regarding financial information and not the provisions regarding health information. Some jurisdictions that have adopted Model # 670 have adopted additional provisions from Model # 672 by bulletin rather than regulation.

IV. Summary of Health Insurance Portability and Accountability Act (HIPAA)

In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA), which, among other things, authorized the U.S. Department of Health and Human Services to promulgate regulations governing consumer privacy protections. The HIPAA Privacy Rule was finalized in 2000. The rule applies to health plans and health care providers, restricting the permitted uses and disclosure of protected health information. HIPAA preempts state law

only to the extent that a covered entity or business associate would find it impossible to comply with both the state and federal requirements.

HIPAA provides individuals the right to access and amend their protected health information, the right to request the restriction of uses and disclosures of protected health information, and the right to receive an accounting of disclosures made to other entities.

A covered entity must obtain the individual's written authorization for any use or disclosure of protected health information that is not for treatment, payment, or health care operations or otherwise permitted or required by the law. A covered entity is also required to provide notice of its privacy practices.

V. Summary of General Data Protection Regulation (GDPR)

The GDPR became effective in May 2018 and applies to U.S. companies if they collect data from citizens of the E.U. over the internet. It requires companies (data "controllers") to obtain explicit consent from consumers to collect their data ("opt in") with an explanation of how the data will be used. It also contains standards for safeguarding the data collected. Under the GDPR, a consumer has the following rights: (1) to receive information about the processing of personal data; (2) to obtain access to the personal data; (3) to request that incorrect, inaccurate or incomplete personal data be corrected; (4) to request that personal data be erased when it is no longer needed or if processing it is unlawful; (5) to object to the processing of personal data for marketing purposes or on grounds relating to a consumer's particular situation; (6) to request the restriction of the processing of personal data in specific cases; (7) to receive personal data in a machine-readable format and the ability to send it to another controller ("data portability"); and (8) to request that decisions based on automated processing concerning the consumer or significantly affecting the consumer and based on consumer's personal data, are made by human beings.

VI. Summary of Recently Adopted Consumer Privacy Protection Laws

A. California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)

In 2018, California became the first U.S. state to adopt a comprehensive privacy law, imposing broad obligations on businesses to provide consumers with transparency and control of their personal data. The California Consumer Privacy Act (CCPA) became effective in 2020. Since it was adopted, it was amended by the California Privacy Rights Act (CPRA), which becomes effective Jan. 1, 2023. Additionally, the California Attorney General promulgated implementing regulations in 2020.

Scope

The CCPA, as amended by the CPRA (California law) applies to companies doing business in California that collect or process consumers' personal information and meet one of the following thresholds: (1) has annual gross revenue in excess of $25,000,000 in the preceding calendar year; (2) annually buys, sells, or shares the personal information of 100,000 or more consumers or households; or (3) derives 50% or more of its annual revenue from selling or sharing consumers' personal information.

Exemptions

The law does not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (GLBA), and its implementing regulations. It also does not apply to protected health information that is governed by the privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services (HHS). Furthermore, this law contains an entity-level exemption for HIPAA-covered entities or business associates governed by the privacy, security, and breach notification rules issued by HHS.

Consumer Rights

California law provides consumers with the following rights : (1) to request deletion of any personal information;[1] (2) to correct inaccurate personal information, taking into account the nature of the personal information and the purposes of the processing of the information; (3) to know about and access the personal information being collected by requesting that the business disclose: the categories and specific pieces of personal information collected, the categories of sources the information was collected from, the business purpose for collecting the information, the categories of third parties with whom the information is shared, and the specific pieces of personal information that was shared; (4) to request the personal information provided by the consumer in a format that is easily understandable, and to the extent technically feasible, in a structured, commonly used, machine-readable format that may also be transmitted to another entity at the consumer's request without hindrance; (5) to know what personal information is sold or shared and to whom; (6) to opt out of the sale or sharing of personal information; (7) to limit the use and disclosure of sensitive personal information; and (7) to not be retaliated against for requesting to opt out or exercise other rights under the law.

Business Obligations

The law imposes the following obligations on all covered businesses: (1) prohibits retaining a consumer's personal information for longer than reasonably necessary for the disclosed purpose; (2) requires implementing reasonable security procedures and practices; (3) requires notice of the following: collection of personal information, including sensitive personal information, retention of information, right to opt out of sale and sharing, and financial incentives; (4) prohibits using sensitive personal information when a consumer has requested not to use or disclose such data.

Enforcement

The CPRA amends the CCPA by placing administrative enforcement authority with the California Privacy Protection Agency, a new state agency created by the CPRA. Under the CPRA, the attorney general retains authority for seeking injunctions and civil penalties. Additionally, if personal information is breached, the consumer can pursue a private civil action against the company.

B. Colorado Privacy Act (CPA)

Scope

The Colorado Privacy Act (CPA) takes effect on July 1, 2023. It applies to entities that conduct business in Colorado or produce or deliver commercial products or services intentionally targeted to residents of Colorado and satisfy one of the following thresholds: (1) controls or processes the personal data of 100,000 or more consumers in a year; or (2) derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of 25,000 or more consumers. The law defines "controllers" as those that "determine the purposes for and means of processing personal data" and defines "processors" as those that "process data on behalf of a controller."

Exemptions

The law contains data-based exemptions (rather than entity-level exemptions) for protected health information collected, processed, or stored by HIPAA-covered entities and their business associates, and information and

[1] And even when information is "deleted," the CCPA right to deletion allows the business to "maintain a confidential record of deletion requests solely for the purpose of preventing the personal information of a consumer who has submitted a deletion request from being sold, for compliance with laws, or for other purposes."

documents created by a HIPAA-covered entity for purposes of complying with HIPAA and its implementing regulations. Additionally, the law contains an exemption for any personal data collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act (GLBA), and implementing regulations, if such collection, processing, sale, or disclosure is in compliance with that law.

Consumer Rights

The CPA provides consumers with the following rights: (1) to opt out of targeted advertising, sale of personal data, and profiling; (2) to confirm whether a controller is processing the consumer's personal data and the right to access such data; (3) to correct inaccuracies in personal data; (4) to delete personal data; and (5) to obtain the personal data in a portable and readily usable format that allows the consumer to transmit the data to another entity.

Business Obligations

The CPA imposes affirmative obligations on controllers, including the following: (1) provide consumers with an accessible, clear, and meaningful privacy notice; (2) specify the express purposes for which personal data are collected and processed; (3) collection of personal data must be adequate, relevant and limited to what is reasonably necessary in relation to the specified purposes; (4) not process personal data for purposes that are not reasonably necessary to or compatible with the specified purposes, without obtaining consent from the consumer; (5) take reasonable measures to secure personal data; (6) not process personal data in violation of any law that prohibits unlawful discrimination; and (7) not process a consumer's sensitive data without first obtaining the consumer's consent. Additionally, controllers are required to enter into contracts with data processors, referencing the responsibilities under the CPA and controllers must conduct a data protection assessment prior to any processing activities that have a heightened risk of harm to consumers.

Enforcement

The CPA does not contain a private right of action but provides the state attorney general and district attorneys authority to take action against entities for violations.

C. Virginia Consumer Data Protection Act (CDPA)

Scope

The Virginia Consumer Data Protection Act (CDPA) becomes effective Jan. 1, 2023. It applies to entities that conduct business in Virginia or produce products or services targeted to Virginia residents when they control or process personal data of at least 100,000 consumers or control or process personal data of at least 25,000 consumers and also derive over 50% of gross revenue from the sale of personal data.

Exemptions

The law contains entity-level exemptions for those subject to GLBA and HIPAA. It specifically exempts financial institutions and data subject to GLBA, and covered entities or business associates governed by the privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services. It also exempts protected health information under HIPAA.

Consumer Rights

The CDPA provides consumers with the following rights: (1) to confirm whether or not a controller is processing the consumer's personal data and if so, to provide the right to access such personal data; (2) to correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of processing of the

consumer's personal data; (3) to delete personal data provided by or obtained about the consumer; (4) to obtain a copy of the consumer's personal data in a portable and readily usable format that allows the consumer to transmit the data to another controller; and (5) to opt out of the processing of the personal data for purposes of targeted advertising, sale of personal data, and profiling.

Business Obligations

Under the law, controllers have the responsibility to do the following: (1) limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed; (2) not process personal data without consumer consent for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such personal data is processed; (3) establish, implement, and maintain reasonable data security practices to protect personal data; (4) not process personal data in violation of any laws that prohibit unlawful discrimination against consumers and not discriminate against consumers exercising their rights under this law; and (5) not process sensitive data concerning a consumer without obtaining the consumer's consent. In addition, controllers must provide consumers with a reasonably accessible, clear, and meaningful privacy notice. Processing activities undertaken by a processor on behalf of a controller must be governed by a data processing agreement. Controllers also must conduct data protection assessments that evaluate the risks associated with processing activities.

Enforcement

Similar to the Colorado law, the law does not contain a private right of action but provides the state attorney general authority to pursue action against entities for violations.

VII. Summary of Working Group Discussions of Selected Key Points

The working group began discussions Dec. 8, 2019, during the Fall National Meeting with the following minimum consumer privacy protections being considered as appropriate for the business of insurance. These rights were based on the Working Group's proposed 2020 charges and are included in the Working Group's initial 2019 Work Plan:

1. the right to receive notice of an insurer's privacy policies and practices;
2. the right to limit an insurer's disclosure of personal data;
3. the right to have access to personal data used by an insurer;
4. the right to request the correction or amendment of personal data used by an insurer;
5. the right of data ownership; and
6. the right of data portability.

Commented [RB3]: This was not added until Summer of 2021, and was discussed only very briefly. It was not on the comment schedule, and I don't think there were written comments on it.

The Work Plan also said that the Working Group discussions would focus on data privacy (rather than data security) and identify areas within NAIC models and state requirement where consumer data privacy protections might need to be enhanced due to changes in technology. In her Dec. 8 presentation, Jennifer McAdam (NAIC) outlined existing privacy provisions in NAIC models and state insurance laws. She said the difference between data privacy and data security is that data privacy is about how data is being collected and used by businesses; while data security is about how data that a business has already collected and has in its possession~~)~~ is stored and protected from unauthorized access. She said the two are often conflated and there are some laws that address both – like GDPR, for example. Furthermore, as many comments have noted, the two issues overlap because a breach of security often results in a loss of privacy. Ms. McAdam said the CCPA is an example of a data privacy law that governs how businesses collect and use consumer data; the rights consumers have to know how that data is being used; the rights consumers have to challenge the accuracy of the data; and how it is being used. Data privacy laws are focused on legal protections for data and consumer rights: In comparison, data security laws, such as the NAIC's Insurance Data Security Model Law

(#668), require operational and technological protections sufficient to ensure that the legal protections are meaningful. Ms. McAdam explained that Model #668 governs how businesses protect the data once it has been collected as well as what businesses need to do if those protections fail as the result of a data breach or other cybersecurity event.

State insurance regulators were concerned about the consumer data that insurers were already presenting in rate filings that had ballooned up to thousands of pages of different data points being gathered by insurers on consumers. They have also seen an increased reliance on third-party risk scores that aggregate consumer information in order to make determinations and conclusions about that information. Regulators noted that insurers have a responsibility to ensure that the third parties used are following state laws and complying with the state's standards for accuracy and fairness. In addition to providing disclosure of the third parties used by insurers when consumers request it, insurers are required to report how the information was gathered; where it was drawn from (e.g., web traffic, geolocation data, social media, etc.); and why the company thinks it needs to use those particular data points as the possibilities available to insurers are endless.

Industry asked the Working Group to consider: 1) Workability by allowing for various exemptions for operational and other reasons that acknowledge vital business purposes for insurers to collect, use, and disclose information. For example, Article IV of the NAIC Model #672 was developed to implement the GLBA, and the exceptions embedded into Section 13 of Model #672 are instructive as to the types of operational functions that need to be preserved and facilitated; 2) Exclusivity by avoiding dual regulation, so insurers are not simultaneously subject to potentially inconsistent or conflicting interpretations by more than one regulator; 3) Clarity by asking that care be taken to consider how best to dovetail with existing models/–laws/regulations; consulting other resources and educating legislators on how privacy bill language impacts the insurance industry, including the legal requirements to retain and use certain data, as well as data mandates; 4) an effective date that allows advance time (like the two to five years that was afforded under the GDPR) for insurers to be ready for implementation, to avoid having piecemeal revisions like the CCPA and the GDPR, as well as a roll-out period with different dates for different provisions within that time frame as a more measured approach to undertake such a significant endeavor.

Consumer Representatives asked the Working Group to consider that: 1) Data vendors are scraping personal consumer information from public sources to produce consumer profiles, scores, and other tools for insurers. The data vendor products, while assembled from public information, raise concerns over consumers' digital rights and privacy; 2) Many data vendors and many types of personal consumer information are not subject to FCRA consumer protections. In turn, many of the types of data and algorithms used by insurers are not subject to either FCRA consumer protections (even though they are the functional equivalent of a consumer report) or the NAIC model law/regulation protections; 3) It is unclear whether the NAIC models cover the new types of data being generated by consumers as part of, or related to, insurance transactions. For example, consumers are producing large volumes of data through telematics programs from devices collecting personal consumer data in the vehicle or home or through wearable devices; 4) There are a lots of organizations working on consumer digital rights (such as the Center for Digital Democracy, the Electronic Privacy Information Center, the Electronic Frontier Foundation, the Public Knowledge-Privacy Rights Clearinghouse, the Public Citizen, the U.S. Public Interest Research Group, and the World Privacy Forum) from whom input and presentations at Working Group meetings should be solicited; and 5) If consumer disclosures are to be used, that the disclosure should be a compliance or enforcement tool that would be created using consumer focus testing and established best practices for the creation of such consumer disclosures.

The COVID-19 pandemic slowed down the Working Group's discussions in 2020; however, discussions continued through seven virtual meetings and two regulator-only meetings of subject matter experts as areas of concentration were being narrowed leading to the Working Group requesting additional guidance from its parent committee.

Commented [RB4]: When were these meetings, and who were the subject matter experts? Were any votes taken?

In April 2021, the Working Group's discussions were redirected to six consumer data privacy rights or types of consumer data privacy protections based on the specific examples identified in item 1.c. of the NAIC Member Adopted Strategy for Consumer Data Privacy Protections received through its parent Committee, the Market Regulation and Consumer Affairs (D) Committee. The Working Group's task was to comment on the following consumer privacy rights concerning consumers' personal information as a basis for a privacy protection framework for the insurance industry (not just health insurance):

1. Right to opt out of data sharing;
2. Right to limit data sharing unless the consumer opts in;
3. Right to correct information;
4. Right to delete information;
5. Right to data portability;
6. Right to restrict the use of data.

Consequently, the Working Group was also tasked with analyzing or determining how insurers were protecting these rights – either to comply with state or federal statutory or regulatory requirements, or on their own initiative or through the adoption of voluntary standards. In 2021, the Working Group met ten times and the regulator only subject matter experts met nine times.

Prior to the 2021 Summer National Meeting, Working Group discussions focused on discussion of, and input on, the following key points from regulators, industry, and consumers for each of the six consumer privacy data rights noted above: definition; examples; consumer risk/impact; current state and federal laws/rules; insurer/licensee impact; actions necessary/insurer obligations to minimize consumer harm; and recommendations. Suggestions that separate privacy requirements be established for each line of business were discussed, but there was consensus that they did not seem to be feasible, as different consumer data privacy requirements across lines of business would limit both consumer protections and understanding.

It was noted during Working Group discussions that insurers utilize third party vendors as sources of data collection and that such vendors may not be subject to regulation by state insurance departments. Regulators stated that the insurers they regulate bear the responsibility for compliance with state insurance privacy requirements. Insurers felt they could not be held responsible because they did not know how such vendors collected or used consumer data and had no way to control the vendors business activities. Regulators and consumer representatives expressed different opinions indicating that insurers' contracts with such vendors could and should be written to require vendors and insurers maintain compliance with insurance regulations regarding consumer data privacy.

During the 2021 Summer National Meeting, NAIC members further recommended that the Working Group's discussion be expanded to include the issue of consumer data ownership.

Working Group discussions revealed that state insurance regulators and consumer representatives believe consumers own the data that is collected and used by the insurance industry to market, sell, and issue insurance policies. It was felt that the type of data collected (name, age, date of birth, height, weight, income, physical condition, personal habits, etc.) describes who a person is and distinguishes one person from another by its very nature. When a consumer shares their data with an insurance company, it is with the understanding that the consumer is letting the company borrow it for a time to determine what insurance rates and insurance coverage the consumer needs. The consumer is not giving up their data to an insurer so it can be sold or given to other organizations from whom the consumer is not seeking insurance coverage, or any other product. Consumer representatives indicated that this practice had happened when they did an online search for insurance rates on health plans. As a result, the consumer representative received hundreds of cold calls from companies selling products other than insurance. When the consumer representative asked with whom the insurance company shared his data, the company sent him a list of 1,700 companies – none of which sold insurance.

Commented [RB5]: Again, when were these meetings and who were the participants? Were any decisions reached?

Commented [RB6]: We'd suggest that beginning here and going forward, these be referred to as "protections" or "issues" to avoid the confusion that may result to consumers and others as to what their actual legal rights might be.

Commented [RB7]: HIPAA and a variety of state laws would likely apply to this situation. It does not indicate a need for new law; rather, enforcement of current law. Was a complaint submitted against the company in question? If not, why not?

The privacy policy statement in Appendix A is designed to be the foundation for the minimum consumer data privacy protections that are appropriate for the business of insurance to be applied to NAIC model #672 as revisions. It is intended to kick start the next step in creating revisions by defining the parameters of the existing consumer data privacy rights; by suggesting definitions and by showing examples of consumer risks. Further discussion is necessary, however, to clarify consumer data privacy rights that may not be fully protected in federal laws or fully covered under NAIC Model laws, and to decide how to provide appropriate protections.

VIII. Conclusion and Recommendations

Months of detailed discussions with regulator, industry, and consumer stakeholders, and the comments they have submitted, have led the Working Group to determine that the *NAIC Insurance Information and Privacy Protection Model Act (Model #670)* and the *Privacy of Consumer Financial and Health Information Regulation (Model #672)* have in the past provided an effective regulatory framework for consumer privacy protections to oversee and enforce consumer data privacy as required by state and federal statutes and regulation. However, these models were adopted by the NAIC 20 and 40 years ago, respectively; with only 17 jurisdictions adopting Model #670.

In consideration of the many changes that have occurred in recent years, as well as the rate of increase in the use of new technologies (AI, machine learning, accelerated underwriting, rating algorithms, etc.), and big data by insurers, the Working Group recommends that models ~~670 and~~ 672 be amended to ensure that regulators can continue to provide consumer data privacy protections essential to meet the consumer data privacy challenges presented by the public use of technology and data by insurers in today's business environment.

The Working Group also recommends the NAIC's Market Regulation Handbook be updated, as necessary, to provide guidance to state insurance regulators so they can verify insurers' compliance the regulatory framework for consumer privacy protections.

Commented [RB8]: There is no need to amend Model 670. It has been only lightly adopted and should be shelved. The Working Group agreed months ago that 672 would be the foundation of any efforts to amend a model or create a new one, and we'd recommend sticking with that position. This inclusion of #670 also conflicts with the first sentence on this page 12, above.

Appendix A

National Association of Insurance Commissioners
Policy Statement on Consumer Data Privacy Protections

Because the business operations of insurance companies are dependent upon the collection and use of personal information and data, state insurance regulators have long understood the need to balance an insurance company's need to collect consumer information and data with the consumer's right to limit the collection and use of data.

The NAIC adopted the *Insurance Information and Privacy Protection Model Act* (Model #670) in 1980 to establish standards for the collection, use and disclosure of information gathered in connection with insurance transactions. A key aspect of this model is that it establishes a regulatory framework for consumers to (1) ascertain what information is being or has been collected about them in connection with insurance transactions; (2) obtain access to such information for the purpose of verifying or disputing its accuracy; (3) limit the disclosure of information collected in connection with insurance transactions; and (4) obtain the reasons for any adverse underwriting decision. This regulatory framework is facilitated through a requirement that insurers or agents provide a written notice to all applicants and policyholders regarding the insurer's information practices.

The NAIC adopted the *Privacy of Consumer Financial and Health Information Model Regulation* (Model #672) in 2000. The model regulation was drafted to implement the requirements set forth in Title V of the federal *Gramm-Leach-Bliley Act* (P.L. 106-102) of 1999 (GLBA). GLBA imposed privacy and security standards on financial institutions and directed state insurance commissioners to adopt certain data privacy and data security regulations. The model also contains provisions governing protection of health information that were taken directly from the Health Insurance Portability and Accountability Act Privacy Rule promulgated by HHS. The NAIC model regulation requires insurers to: (1) notify consumers about their privacy policies; (2) give consumers the opportunity to prohibit the sharing of their protected financial information with non-affiliated third parties; and (3) obtain affirmative consent from consumers before sharing protected health information with any other parties, affiliates, and non-affiliates. The key difference between the treatment of financial information and health information is that insurers must give consumers the right (with limited exceptions) to "opt out" of the disclosure or sharing of their financial information, but insurers must get explicit authorization ("opt in") before sharing health information.

This policy statement is based on the consumer protections set forth in these two models and serves the purpose of informing licensed insurance entities, consumers, and the other state and federal regulatory agencies on what the NAIC currently supports as the minimum consumer data privacy protections that are appropriate for the business of insurance. The policy statement is not intended to modify any existing NAIC models and does not carry the weight of law or impose any legal obligations in states that have adopted those models.

The policy statement addresses consumer data privacy protections of (1) transparency; (2) consumer control; (3) consumer access; (4) data accuracy; and (5) ~~data ownership and~~ portability. The policy statement intentionally excludes standards for data security and standards for the investigation and notification to an insurance commissioner of a licensed insurance entity's cybersecurity event, which are the subject of separate model laws and interpretive guidance.

The following definitions are used for the purposes of this policy statement.

A. "Adverse Decision" means declination of insurance coverage, termination of insurance coverage, charging a higher rate for insurance coverage, or denying a claim.
B. "Consumer" means an individual who is seeking to obtain, obtaining, or have obtained a product or service from

Commented [RB9]: We'd recommend deleting all of this document. The recommendations of the working group are in Section VIII, Conclusions and Recommendations, and once corrected, they are sufficient. This appendix is not needed.

Commented [RB10]: Duplicative of "consumer control"

Commented [RB11]: What is the source of these definitions? If they come from #670 or #672, it would be helpful if they were sourced by section. Are they consistent with those in the CA, VA, and CO privacy bills?

an insurer. For example, an individual who has submitted an application for insurance is a consumer of the company to which he or she has applied, as is an individual whose policy with the company has expired.

C. "Customer" means a consumer with whom an insurer has an on-going relationship.

D. "Licensee" means any insurer, producer, or other person licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to a state insurance law.

E. "Personal Information" means any individually identifiable information or data gathered in connection with an insurance transaction from which judgments can be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit, health, or any other personal characteristics. Personal information includes:

1. "Non-Public Personal Information," which means information that a consumer provides to a licensee to obtain an insurance product or service (like income, credit history, name and address); information about a consumer a licensee has as a result of a transaction involving an insurance product or service (like premium payment history, how much a life insurance policy is worth, and the value of personal property insured); and all other information about a consumer that a licensee uses in connection with providing a product or service to a consumer.
2. "Non-public personal health information," which means any information that identifies a consumer in some way, and includes information about a consumer's health, including past and present physical and mental health, details about health care, and payment for health care.

I. Transparency

A ~~l~~Licensee should provide a clear and conspicuous notice to consumers that accurately reflects its privacy policies and practices when it first requests personal information about the consumer from the consumer or a third party.

A Llicensee should also provide a periodic notice of its privacy policies and practices to customers ~~not less than annually during the continuation of the customer relationship.~~

If a licensee makes an adverse decision based on information/data that was not supplied by the consumer, the licensee should provide the consumer with the specific reasons for the adverse decision.

II. Consumer Control

Licensees should, at a minimum, provide consumers the opportunity to prohibit the sharing of their non-public personal information with third parties, except for specific purposes required or specifically permitted by law. (Opt-Out)

Licensees should obtain affirmative consent from consumers before sharing non-public personal health information with any other entity, including its affiliates and non-affiliates, except for specific purposes or otherwise specifically permitted by law. (Opt-In)

III. Consumer Access

Any consumer should have the right to submit a request to a licensee to obtain access to his/her personal information used by the licensee in its operations. Upon request, the licensee should within 30 business days provide a copy of the consumer's personal information, an explanation on how the personal information was used (i.e., rating, underwriting, claims), and provide the source of the personal information. If personal information is in coded form,

Commented [RB12]: It would be helpful to all users of this document if all of these protections were cross-referenced to their source in the section(s) of the existing model(s).

Commented [RB13]: This is the first of several defined terms that, as such, should probably all be capitalized.

Commented [RB14]: This is not consistent with the FAST Act amendments, which have been incorporated into GLBA and state laws across the country.

the licensee should provide an accurate translation in plain language.

IV. Data Accuracy

Within 30 business days after receiving a request from a consumer to correct, amend, or delete personal information used by the licensee in its operations, the licensee should either make the requested correction, amendment, or deletion or notify the consumer of its refusal to do so, the reasons for the refusal, and the consumer's right to file a statement of dispute setting forth what the consumer thinks is the correct information and the reasons for disagreeing with the licensee.

If the licensee corrects, amends, or deletes personal information, the licensee should notify any person or entity that has received the prior personal information within the last 7 years. If the licensee does not correct, amend, or delete the disputed personal information, the licensee should notify any person or entity that has received the prior personal information within the last 7 years of the consumer's statement of dispute.

V. Data ~~Ownership and~~ Portability

A customer should have the right to request a copy of his/her personal information that he/she has provided to the licensee for use in the licensee's operations. A licensee should provide a customer a copy of his/her personal information within 30 business days of the request. Examples of this type of personal information include telematics data and "Internet of Things" ("IoT") data.

Commented [RB15]: This may not be practical in the health care world.

Commented [RB16]: The meaning of this term is subject to discussion and debate, and until defined, suggest it not be used in this context.

Commented [RB17]: How does this differ from Access, Item III, above? Is it clear?

Commented [RB18]: Suggest that these terms be defined, and examples given of what information an insurer might have from these sources.

December 2, 2021

Cynthia Amann and Ron Kreiter
Privacy Protections Working Group
National Association of Insurance Commissioners
1100 Walnut Street, Suite 1500
Kansas City, MO 64106

Dear Chairwoman Amann and Vice Chairman Kreiter:

On behalf of the Independent Insurance Agents and Brokers of America (IIABA), I write to comment on your working group's consideration of the recently unveiled "Report on Consumer Data Privacy Protections." IIABA opposes the adoption of the report in its current form and urges the working group to either make the necessary revisions (including, most notably, deleting the appendix) or delay the adoption of the report until reasonable consideration of its substantial recommendations can occur. This letter augments the comments IIABA has also submitted in conjunction with the American Property Casualty Insurance Association and the National Association of Mutual Insurance Companies and emphasizes the issues that are of greatest concern to our association.

General Comments and Primary Concern

The most startling and troubling elements of the paper are a recommended series of new industry obligations and mandates that were never discussed, debated, or voted on by the Privacy Protections Working Group. The adoption or endorsement of such public policy recommendations has incredibly significant implications, and it would be presumptive and highly inappropriate to approve this document given the absence of actual consideration. The origin of these recommendations is unknown, and they were only released to the public in recent days. It has been suggested the report is designed to merely document the efforts of the working group and to recommend to your parent committee that the existing NAIC privacy models should be examined and revised where appropriate. There would be little concern among interested parties if the paper was limited in this way, but the reality is the draft extends far beyond these parameters.

There are a variety of other flaws, misstatements, unsubstantiated anecdotes, and references to numerous unannounced regulator-only meetings in the draft report, but the primary concern we have is the specific and unvetted public policy recommendations it makes. If the working group's objective is to "kick start" the discussion about whether and how to revise the existing models and to identify topics especially worth of subsequent consideration, it should so without

preordaining the outcome, making broad statements of policy at this time, and recommending exactly what actions and model amendments should be made. For these reasons, we urge the working group to either (1) remove the appendix and its public policy recommendations because they were never discussed and are unnecessary and unhelpful to the model review process that will follow or (2) delay the adoption of the draft appendix and any recommendations until these specific proposals can actually be properly considered by working group members with the benefit of public comment.

Although IIABA has very strong concerns with the substantive public policy recommendations and model revisions outlined in the draft paper, we should note that the bulk of the draft report is thoughtfully crafted and noncontroversial. Numerous sections of the paper appropriately review and analyze existing NAIC privacy models, federal and international privacy laws, recently enacted state privacy statutes, and the manner in which these regimes apply to different types of insurance licensees. This review should be helpful to state insurance regulators and to this working group or any successor that considers whether and how to revise Models 670 and 672.

Additional Recommendations

IIABA also offers the following recommendations:

I. Introduction

- Delete the last sentence of the first paragraph.

  We propose the deletion of this sentence and its discussion of a "policy statement" for the reasons identified above and because the appendix should itself be deleted.

- Revise the first sentence of the second paragraph in the following way:

  > *"The Working Group discussed how best to balance the need for information by those conducting the business of insurance and the public's need for fairness in insurance information practices ~~rights of insurers to use data for legitimate business purposes with consumers' rights to control what data is used and how it is used~~."*

  We propose this revision because it mirrors the preamble of NAIC Model 670 and because there is no unlimited right of consumers to control what data is used and how it is used. The draft text is imprecise and suggests the existence of broad rights that simply do not exist.

VII. Summary of Working Group Discussions of Selected Key Points

- Revise the final paragraph of this section in the following way:

  > *~~The privacy policy statement in Appendix A is designed to be the foundation for the minimum consumer data privacy protections that are appropriate for the business of insurance to be applied to NAIC model #672 as revisions. It~~ This report is intended to kick start the next step in creating revisions by defining the parameters of the existing consumer data privacy rights~~; by suggesting definitions and by showing examples of consumer risks~~. Further discussion is necessary, however, to clarify consumer data privacy rights that may not be fully*

protected in federal laws or fully covered under NAIC Model laws, and to decide how to provide appropriate protections.

We propose these revisions in light of concerns regarding the unwarranted recommendations identified in the appendix. The modifications we propose also achieve the core objective of the report as articulated by the working group during its most recent meeting (i.e. to call for a review of the existing NAIC models without preordaining specific outcomes).

Appendix A

- Delete the appendix.

  This is the most important revision we propose, and we suggest this because it is unnecessary and for all of the other reasons addressed previously in this letter.

Conclusion

On behalf of the hundreds of thousands of insurance professionals we represent, IIABA thanks you for the opportunity to submit these comments. We look forward to participating in your December 11 meeting and are happy to assist your working group's consideration of these issues in any way you deem appropriate. Please feel free to contact me at 202-302-1607 or via email at wes.bissett@iiaba.net with any questions or if we can assist you in any manner.

Very truly yours,

Wesley Bissett
Senior Counsel, Government Affairs

Privacy Protections (D) Working Group Report on Consumer Data Privacy Protections

Exposure Draft

November 18, 2021

Table of Contents

I. Introduction

The Privacy Protections (D) Working Group was appointed in 2019 to review state insurance privacy protections regarding the collection, use, and disclosure of information gathered in connection with insurance transactions and make recommended changes, as needed, to NAIC models addressing privacy protection. This includes an insurer's use of data collected from a consumer and data supplied to an insurer by a third-party vendor. Rather than focusing on revisions to NAIC models, the main deliverables for 2021 were to set forth a policy statement on the minimum consumer privacy protections that are appropriate for the business of insurance, after taking into consideration the consumer privacy protections that already exist under applicable state and federal laws.

The Working Group discussed how best to balance the rights of insurers to use data for legitimate business purposes with consumers' rights to control what data is used and how it is used. The following privacy protections for consumers were discussed: (1) the right to opt out of data sharing, (2) the right to limit data sharing unless the consumer opts in, (3) the right to correct information, (4) the right to delete information, (5) the right of data portability, (6) the right to restrict the use of data, (7) the right of data ownership, (8) the right of notice, and (9) the right of nondiscrimination / non-retaliation.

The Working Group received comments from the ACLI, AHIP, APCIA, BCBSA, the Coalition of Health Insurers, NAMIC, MLPA, and NAIC consumer representatives Birny Birnbaum, Brenda Cude, Karrol Kitt, and Harry Ting.

II. Overview of Issue

Consumer awareness and regulatory concerns about the use of consumer data by a variety of commercial, financial, and technology companies are increasing. This has led to adoption of the General Data Protection Regulation (GDPR) in the E.U. and the California Consumer Privacy Act (CCPA) and other state data privacy protection laws in the U.S. Though data privacy concerns extend beyond the insurance sector, the increasing use of data and the passage of these new laws is causing the insurance industry and consumer groups alike to pressure Congress to enact federal privacy legislation

While federal legislative efforts are currently stalled due to other legislative priorities and differing perspectives from consumers and industry on the best path forward, it is likely that Congress will begin focusing on the issue again soon. The current pause provides state insurance regulators an opportunity to update state privacy protections consistent with the current insurance business environment and potentially forestall or mitigate the impacts of any preemptive federal legislation. State policymakers have also responded to the privacy debate with varying legislative proposals to provide consumers with greater transparency and control over the use of personal information, with California, Virginia, and Colorado being leading examples. These comprehensive state data privacy laws each have either entity-level or data-level exemptions for entities subject to or information collected pursuant to the federal Gramm-Leach-Bliley Act (GLBA) and/or the privacy regulations adopted under the Health Insurance Portability and Accountability Act (HIPAA).

III. Summary of Consumer Privacy Protections Provided by NAIC Model Laws

The NAIC has three model laws governing data privacy: *Health Information Privacy Model Act* (Model #55); *NAIC Insurance Information and Privacy Protection Model Act* (#670) and *Privacy of Consumer Financial and Health Information Regulation* (#672), each of which is based upon or influenced by federal privacy laws. The NAIC's Model #670 contains many of the consumer rights found in these comprehensive state laws, which can be traced back to the Fair Credit Reporting Act (FCRA). And Model #672 is based, in large part, on GLBA and the HIPAA regulations. Generally, insurers and other entities licensed by state departments of insurance are carved out of more comprehensive state laws of general applicability. Because of this, insurance regulators must be aware when new protections are

added to laws applicable to other businesses, especially when they address new technologies and ways consumer information is collected and shared, so that comparable protection can be added, as necessary, to the laws governing the insurance industry. Of note, GLBA and HIPAA each set a federal floor for the entities within their scope, from which states can build upon. This is what the NAIC did in drafting the *Health Information Privacy Model Act* (Model #55) and the *Privacy of Consumer Financial and Health Information Regulation* (#672). GLBA applies to the entire insurance industry HPAA applies to the health insurance sector.

A. NAIC Insurance Information and Privacy Protection Model Act (Model #670)

The NAIC adopted the *NAIC Insurance Information and Privacy Protection Model Act* (#670) in 1980 following federal enactment of the Fair Credit Reporting Act in 1970 and the Federal Privacy Act in 1974. This model act establishes standards for the collection, use and disclosure of information gathered in connection with insurance transactions by insurance companies, insurance producers and insurance support organizations.

A key aspect of this model is that it establishes a regulatory framework for consumers to (1) ascertain what information is being or has been collected about them in connection with insurance transactions; (2) obtain access to such information for the purpose of verifying or disputing its accuracy; (3) limit the disclosure of information collected in connection with insurance transactions; and (4) obtain the reasons for any adverse underwriting decision.

This regulatory framework is facilitated through a requirement that insurers or agents provide a written notice to all applicants and policyholders regarding the insurer's information practices. The notice must address the following: (1) whether personal information may be collected from persons other than the individual or individuals seeking insurance coverage; (2) the types of personal information that may be collected, the types of sources and investigative techniques that may be used to collect such information; (3) the types of disclosures allowed under the law; (4) a description of the rights established under the law; and (5) notice that information obtained from a report prepared by an insurance support organization may be retained by the insurance support organization and disclosed to other persons.

Of note, the model prohibits disclosure of any personal information about an individual collected or received in connection with an insurance transaction without the individual's written authorization, subject to limited exceptions. However, some categories of information may be disclosed for marketing purposes if the consumer "has been given an opportunity to indicate that he or she does not want personal information disclosed for marketing purposes and has given no indication that he or she does not want the information disclosed," It also provides consumers with the right to request that an insurer provide access to recorded personal information, disclose the identity of the third parties to whom the insurance company disclosed information (if recorded); disclose the source of collected information (if available); and provide procedures by which the consumer may request correction, amendment, or deletion of recorded personal information.

Seventeen states have adopted Model #670: AZ, CA, CT, GA, HI, IL, KS, MA, ME, MN, MT, NV, NJ, NC, OH, OR, and VA.

B. NAIC Health Information Privacy Model Act (Model #55)

The NAIC adopted the *Health Information Privacy Model Act* (Model #55) following federal adoption of the privacy regulations authorized by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

This model sets standards to protect health information from unauthorized collection, use and disclosure by requiring insurance companies to establish procedures for the treatment of all health information by all insurance carriers. The drafters of Model #55 believed it was important that the same rules apply to all lines of insurance, since health

insurance carriers are not the only ones that use health information to transact their business. For example, health information is necessary for life insurance underwriting, and often essential to property and casualty insurers in settling workers' compensation claims and personal injury liability claims. Reinsurers also use protected health information to write reinsurance.

The model requires carriers to develop and implement written policies, standards, and procedures for the management of health information, including to guard against the unauthorized collection, use or disclosure of protected health information. It provides consumers with the right to access their protected health information and amend any inaccuracies. The model also requires insurers to obtain written authorization ("opt-in") before collecting, using, or disclosing protected health information, except when performing limited activities.

Many of the provisions found in Model #55 were later incorporated into the *Privacy of Consumer Financial and Health Information Regulation* (Model #672).

The following 13 jurisdictions have adopted legislation related to Model #55: CA, CO, DE, KY, LA, ME, MO, ND, RI, SD, TX.

C. NAIC Privacy of Consumer Financial and Health Information Regulation (Model #672)

The NAIC adopted the *Privacy of Consumer Financial and Health Information Model Regulation (Model #672)* in 2000. The model regulation was drafted to implement the requirements set forth in Title V of GLBA. GLBA imposed privacy and security standards on financial institutions, defined to include insurers and other insurance licensees, and directed state insurance commissioners to adopt certain data privacy and data security regulations. The provisions governing protection of financial information are based on privacy regulations promulgated by federal banking agencies. The model also contains provisions governing protection of health information that were taken directly from Model #55 and from the HIPAA Privacy Rule promulgated by HHS.

The model regulation provides protection for financial and health information about consumers held by insurance companies, agents, and other entities engaged in insurance activities. In general, the model regulation requires insurers to: (1) notify consumers about their privacy policies; (2) give consumers the opportunity to prohibit the sharing of their protected financial information with non-affiliated third parties; and (3) obtain affirmative consent from consumers before sharing protected health information with any other parties, affiliates, and non-affiliates.

The key difference between the treatment of financial information and health information is that insurers must give consumers the right to "opt out" of the disclosure or sharing of their financial information but insurers must obtain explicit authorization from the consumer ("opt-in") before sharing health information. Every jurisdiction has a version of this model regulation, although nineteen jurisdictions have only adopted the provisions regarding financial information and not the provisions regarding health information. Some jurisdictions that have adopted Model # 670 have adopted additional provisions from Model # 672 by bulletin rather than regulation.

IV. Summary of Health Insurance Portability and Accountability Act (HIPAA)

In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA), which, among other things, authorized the U.S. Department of Health and Human Services to promulgate regulations governing consumer privacy protections. The HIPAA Privacy Rule was finalized in 2000. The rule applies to health plans and health care providers, restricting the permitted uses and disclosure of protected health information. HIPAA preempts state law

only to the extent that a covered entity or business associate would find it impossible to comply with both the state and federal requirements.

HIPAA provides individuals the right to access and amend their protected health information, the right to request the restriction of uses and disclosures of protected health information, and the right to receive an accounting of disclosures made to other entities.

A covered entity must obtain the individual's written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care operations or otherwise permitted or required by the law. A covered entity is also required to provide notice of its privacy practices.

V. Summary of General Data Protection Regulation (GDPR)

The GDPR became effective in May 2018 and applies to U.S. companies if they collect data from citizens of the E.U. over the internet. It requires companies (data "controllers") to obtain explicit consent from consumers to collect their data ("opt in") with an explanation of how the data will be used. It also contains standards for safeguarding the data collected. Under the GDPR, a consumer has the following rights: (1) to receive information about the processing of personal data; (2) to obtain access to the personal data; (3) to request that incorrect, inaccurate or incomplete personal data be corrected; (4) to request that personal data be erased when it is no longer needed or if processing it is unlawful; (5) to object to the processing of personal data for marketing purposes or on grounds relating to a consumer's particular situation; (6) to request the restriction of the processing of personal data in specific cases; (7) to receive personal data in a machine-readable format and the ability to send it to another controller ("data portability"); and (8) to request that decisions based on automated processing concerning the consumer or significantly affecting the consumer and based on consumer's personal data, are made by human beings.

VI. Summary of Recently Adopted Consumer Privacy Protection Laws

A. California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)

In 2018, California became the first U.S. state to adopt a comprehensive privacy law, imposing broad obligations on businesses to provide consumers with transparency and control of their personal data. The California Consumer Privacy Act (CCPA) became effective in 2020. Since it was adopted, it was amended by the California Privacy Rights Act (CPRA), which becomes effective Jan. 1, 2023. Additionally, the California Attorney General promulgated implementing regulations in 2020.

Scope

The CCPA, as amended by the CPRA (California law) applies to companies doing business in California that collect or process consumers' personal information and meet one of the following thresholds: (1) has annual gross revenue in excess of $25,000,000 in the preceding calendar year; (2) annually buys, sells, or shares the personal information of 100,000 or more consumers or households; or (3) derives 50% or more of its annual revenue from selling or sharing consumers' personal information.

Exemptions

The law does not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (GLBA), and its implementing regulations. It also does not apply to protected health information that is governed by the privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services (HHS). Furthermore, this law contains an entity-level exemption for HIPAA-covered entities or business associates governed by the privacy, security, and breach notification rules issued by HHS.

Consumer Rights

California law provides consumers with the following rights : (1) to request deletion of any personal information;[1] (2) to correct inaccurate personal information, taking into account the nature of the personal information and the purposes of the processing of the information; (3) to know about and access the personal information being collected by requesting that the business disclose: the categories and specific pieces of personal information collected, the categories of sources the information was collected from, the business purpose for collecting the information, the categories of third parties with whom the information is shared, and the specific pieces of personal information that was shared; (4) to request the personal information provided by the consumer in a format that is easily understandable, and to the extent technically feasible, in a structured, commonly used, machine-readable format that may also be transmitted to another entity at the consumer's request without hindrance; (5) to know what personal information is sold or shared and to whom; (6) to opt out of the sale or sharing of personal information; (7) to limit the use and disclosure of sensitive personal information; and (7) to not be retaliated against for requesting to opt out or exercise other rights under the law.

Business Obligations

The law imposes the following obligations on all covered businesses: (1) prohibits retaining a consumer's personal information for longer than reasonably necessary for the disclosed purpose; (2) requires implementing reasonable security procedures and practices; (3) requires notice of the following: collection of personal information, including sensitive personal information, retention of information, right to opt out of sale and sharing, and financial incentives; (4) prohibits using sensitive personal information when a consumer has requested not to use or disclose such data.

Enforcement

The CPRA amends the CCPA by placing administrative enforcement authority with the California Privacy Protection Agency, a new state agency created by the CPRA. Under the CPRA, the attorney general retains authority for seeking injunctions and civil penalties. Additionally, if personal information is breached, the consumer can pursue a private civil action against the company.

B. Colorado Privacy Act (CPA)

Scope

The Colorado Privacy Act (CPA) takes effect on July 1, 2023. It applies to entities that conduct business in Colorado or produce or deliver commercial products or services intentionally targeted to residents of Colorado and satisfy one of the following thresholds: (1) controls or processes the personal data of 100,000 or more consumers in a year; or (2) derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of 25,000 or more consumers. The law defines "controllers" as those that "determine the purposes for and means of processing personal data" and defines "processors" as those that "process data on behalf of a controller."

Exemptions

The law contains data-based exemptions (rather than entity-level exemptions) for protected health information collected, processed, or stored by HIPAA-covered entities and their business associates, and information and

[1] And even when information is "deleted," the CCPA right to deletion allows the business to "maintain a confidential record of deletion requests solely for the purpose of preventing the personal information of a consumer who has submitted a deletion request from being sold, for compliance with laws or for other purposes."

documents created by a HIPAA-covered entity for purposes of complying with HIPAA and its implementing regulations. Additionally, the law contains an exemption for any personal data collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act (GLBA), and implementing regulations, if such collection, processing, sale, or disclosure is in compliance with that law.

Consumer Rights

The CPA provides consumers with the following rights: (1) to opt out of targeted advertising, sale of personal data, and profiling; (2) to confirm whether a controller is processing the consumer's personal data and the right to access such data; (3) to correct inaccuracies in personal data; (4) to delete personal data; and (5) to obtain the personal data in a portable and readily usable format that allows the consumer to transmit the data to another entity.

Business Obligations

The CPA imposes affirmative obligations on controllers, including the following: (1) provide consumers with an accessible, clear, and meaningful privacy notice; (2) specify the express purposes for which personal data are collected and processed; (3) collection of personal data must be adequate, relevant and limited to what is reasonably necessary in relation to the specified purposes; (4) not process personal data for purposes that are not reasonably necessary to or compatible with the specified purposes, without obtaining consent from the consumer; (5) take reasonable measures to secure personal data; (6) not process personal data in violation of any law that prohibits unlawful discrimination; and (7) not process a consumer's sensitive data without first obtaining the consumer's consent. Additionally, controllers are required to enter into contracts with data processors, referencing the responsibilities under the CPA and controllers must conduct a data protection assessment prior to any processing activities that have a heightened risk of harm to consumers.

Enforcement

The CPA does not contain a private right of action but provides the state attorney general and district attorneys authority to take action against entities for violations.

C. Virginia Consumer Data Protection Act (CDPA)

Scope

The Virginia Consumer Data Protection Act (CDPA) becomes effective Jan. 1, 2023. It applies to entities that conduct business in Virginia or produce products or services targeted to Virginia residents when they control or process personal data of at least 100,000 consumers or control or process personal data of at least 25,000 consumers and also derive over 50% of gross revenue from the sale of personal data.

Exemptions

The law contains entity-level exemptions for those subject to GLBA and HIPAA. It specifically exempts financial institutions and data subject to GLBA, and covered entities or business associates governed by the privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services. It also exempts protected health information under HIPAA.

Consumer Rights

The CDPA provides consumers with the following rights: (1) to confirm whether or not a controller is processing the consumer's personal data and if so, to provide the right to access such personal data; (2) to correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of processing of the

consumer's personal data; (3) to delete personal data provided by or obtained about the consumer; (4) to obtain a copy of the consumer's personal data in a portable and readily usable format that allows the consumer to transmit the data to another controller; and (5) to opt out of the processing of the personal data for purposes of targeted advertising, sale of personal data, and profiling.

Business Obligations

Under the law, controllers have the responsibility to do the following: (1) limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed; (2) not process personal data without consumer consent for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such personal data is processed; (3) establish, implement, and maintain reasonable data security practices to protect personal data; (4) not process personal data in violation of any laws that prohibit unlawful discrimination against consumers and not discriminate against consumers exercising their rights under this law; and (5) not process sensitive data concerning a consumer without obtaining the consumer's consent. In addition, controllers must provide consumers with a reasonably accessible, clear, and meaningful privacy notice. Processing activities undertaken by a processor on behalf of a controller must be governed by a data processing agreement. Controllers also must conduct data protection assessments that evaluate the risks associated with processing activities.

Enforcement

Similar to the Colorado law, the law does not contain a private right of action but provides the state attorney general authority to pursue action against entities for violations.

VII. Summary of Working Group Discussions of Selected Key Points

The working group began discussions Dec. 8, 2019, during the Fall National Meeting with the following minimum consumer privacy protections being considered as appropriate for the business of insurance. These rights were based on the Working Group's proposed 2020 charges and are included in the Working Group's initial 2019 Work Plan:

1. the right to receive notice of an insurer's privacy policies and practices;
2. the right to limit an insurer's disclosure of personal data;
3. the right to have access to personal data used by an insurer;
4. the right to request the correction or amendment of personal data used by an insurer;
5. the right of data ownership; and
6. the right of data portability.

The Work Plan also said that the Working Group discussions would focus on data privacy (rather than data security) and identify areas within NAIC models and state requirement where consumer data privacy protections might need to be enhanced due to changes in technology. In her Dec. 8 presentation, Jennifer McAdam (NAIC) outlined existing privacy provisions in NAIC models and state insurance laws. She said the difference between data privacy and data security is that data privacy is about how data is being collected and used by businesses; while data security is about how data that a business has already collected and has in its possession) is stored and protected from unauthorized access. She said the two are often conflated and there are some laws that address both – like GDPR, for example. Furthermore, as many comments have noted, the two issues overlap because a breach of security often results in a loss of privacy. Ms. McAdam said the CCPA is an example of a data privacy law that governs how businesses collect and use consumer data; the rights consumers have to know how that data is being used; the rights consumers have to challenge the accuracy of the data; and how it is being used. Data privacy laws are focused on legal protections for data and consumer rights: In comparison, data security laws, such as the NAIC's Insurance Data Security Model Law

(#668), require operational and technological protections sufficient to ensure that the legal protections are meaningful. Ms. McAdam explained that Model #668 governs how businesses protect the data once it has been collected as well as what businesses need to do if those protections fail as the result of a data breach or other cybersecurity event.

State insurance regulators were concerned about the consumer data that insurers were already presenting in rate filings that had ballooned up to thousands of pages of different data points being gathered by insurers on consumers. They have also seen an increased reliance on third-party risk scores that aggregate consumer information in order to make determinations and conclusions about that information. Regulators noted that insurers have a responsibility to ensure that the third parties used are following state laws and complying with the state's standards for accuracy and fairness. In addition to providing disclosure of the third parties used by insurers when consumers request it, insurers are required to report how the information was gathered; where it was drawn from (e.g., web traffic, geolocation data, social media, etc.); and why the company thinks it needs to use those particular data points as the possibilities available to insurers are endless.

Industry asked the Working Group to consider: 1) Workability by allowing for various exemptions for operational and other reasons that acknowledge vital business purposes for insurers to collect, use, and disclose information. For example, Article IV of the NAIC Model #672 was developed to implement the GLBA, and the exceptions embedded into Section 13 of Model #672 are instructive as to the types of operational functions that need to be preserved and facilitated; 2) Exclusivity by avoiding dual regulation, so insurers are not simultaneously subject to potentially inconsistent or conflicting interpretations by more than one regulator; 3) Clarity by asking that care be taken to consider how best to dovetail with existing models/ laws/regulations; consulting other resources and educating legislators on how privacy bill language impacts the insurance industry, including the legal requirements to retain and use certain data, as well as data mandates; 4) an effective date that allows advance time (like the two to five years that was afforded under the GDPR) for insurers to be ready for implementation, to avoid having piecemeal revisions like the CCPA and the GDPR, as well as a roll-out period with different dates for different provisions within that time frame as a more measured approach to undertake such a significant endeavor.

Consumer Representatives asked the Working Group to consider that: 1) Data vendors are scraping personal consumer information from public sources to produce consumer profiles, scores, and other tools for insurers. The data vendor products, while assembled from public information, raise concerns over consumers' digital rights and privacy; 2) Many data vendors and many types of personal consumer information are not subject to FCRA consumer protections. In turn, many of the types of data and algorithms used by insurers are not subject to either FCRA consumer protections (even though they are the functional equivalent of a consumer report) or the NAIC model law/regulation protections; 3) It is unclear whether the NAIC models cover the new types of data being generated by consumers as part of, or related to, insurance transactions. For example, consumers are producing large volumes of data through telematics programs from devices collecting personal consumer data in the vehicle or home or through wearable devices; 4) There are a lots of organizations working on consumer digital rights (such as the Center for Digital Democracy, the Electronic Privacy Information Center, the Electronic Frontier Foundation, the Public Knowledge-Privacy Rights Clearinghouse, the Public Citizen, the U.S. Public Interest Research Group, and the World Privacy Forum) from whom input and presentations at Working Group meetings should be solicited; and 5) If consumer disclosures are to be used, that the disclosure should be a compliance or enforcement tool that would be created using consumer focus testing and established best practices for the creation of such consumer disclosures.

The COVID-19 pandemic slowed down the Working Group's discussions in 2020; however, discussions continued through seven virtual meetings and two regulator-only meetings of subject matter experts as areas of concentration were being narrowed leading to the Working Group requesting additional guidance from its parent committee.

In April 2021, the Working Group's discussions were redirected to six consumer data privacy rights or types of consumer data privacy protections based on the specific examples identified in item 1.c. of the NAIC Member Adopted Strategy for Consumer Data Privacy Protections received through its parent Committee, the Market Regulation and Consumer Affairs (D) Committee. The Working Group's task was to comment on the following consumer privacy rights concerning consumers' personal information as a basis for a privacy protection framework for the insurance industry (not just health insurance):

1. Right to opt out of data sharing;
2. Right to limit data sharing unless the consumer opts in;
3. Right to correct information;
4. Right to delete information;
5. Right to data portability;
6. Right to restrict the use of data.

Consequently, the Working Group was also tasked with analyzing or determining how insurers were protecting these rights – either to comply with state or federal statutory or regulatory requirements, or on their own initiative or through the adoption of voluntary standards. In 2021, the Working Group met ten times and the regulator only subject matter experts met nine times.

Prior to the 2021 Summer National Meeting, Working Group discussions focused on discussion of, and input on, the following key points from regulators, industry, and consumers for each of the six consumer privacy data rights noted above: definition; examples; consumer risk/impact; current state and federal laws/rules; insurer/licensee impact; actions necessary/insurer obligations to minimize consumer harm; and recommendations. Suggestions that separate privacy requirements be established for each line of business were discussed, but there was consensus that they did not seem to be feasible, as different consumer data privacy requirements across lines of business would limit both consumer protections and understanding.

It was noted during Working Group discussions that insurers utilize third party vendors as sources of data collection and that such vendors may not be subject to regulation by state insurance departments. Regulators stated that the insurers they regulate bear the responsibility for compliance with state insurance privacy requirements. Insurers felt they could not be held responsible because they did not know how such vendors collected or used consumer data and had no way to control the vendors business activities. Regulators and consumer representatives expressed different opinions indicating that insurers' contracts with such vendors could and should be written to require vendors and insurers maintain compliance with insurance regulations regarding consumer data privacy.

During the 2021 Summer National Meeting, NAIC members further recommended that the Working Group's discussion be expanded to include the issue of consumer data ownership.

Working Group discussions revealed that state insurance regulators and consumer representatives believe consumers own the data that is collected and used by the insurance industry to market, sell, and issue insurance policies. It was felt that the type of data collected (name, age, date of birth, height, weight, income, physical condition, personal habits, etc.) describes who a person is and distinguishes one person from another by its very nature. When a consumer shares their data with an insurance company, it is with the understanding that the consumer is letting the company borrow it for a time to determine what insurance rates and insurance coverage the consumer needs. The consumer is not giving up their data to an insurer so it can be sold or given to other organizations from whom the consumer is not seeking insurance coverage, or any other product. Consumer representatives indicated that this practice had happened when they did an online search for insurance rates on health plans. As a result, the consumer representative received hundreds of cold calls from companies selling products other than insurance. When the consumer representative asked with whom the insurance company shared his data, the company sent him a list of 1,700 companies – none of which sold insurance.

The privacy policy statement in Appendix A is designed to be the foundation for the minimum consumer data privacy protections that are appropriate for the business of insurance to be applied to NAIC model #672 as revisions. It is intended to kick start the next step in creating revisions by defining the parameters of the existing consumer data privacy rights; by suggesting definitions and by showing examples of consumer risks. Further discussion is necessary, however, to clarify consumer data privacy rights that may not be fully protected in federal laws or fully covered under NAIC Model laws, and to decide how to provide appropriate protections.

VIII. Conclusion and Recommendations

Months of detailed discussions with regulator, industry, and consumer stakeholders, and the comments they have submitted, have led the Working Group to determine that the *NAIC Insurance Information and Privacy Protection Model Act (Model #670)* and the *Privacy of Consumer Financial and Health Information Regulation (Model #672)* have in the past provided an effective regulatory framework for consumer privacy protections to oversee and enforce consumer data privacy as required by state and federal statutes and regulation. However, these models were adopted by the NAIC 20 and 40 years ago, respectively; with only 17 jurisdictions adopting Model #670.

In consideration of the many changes that have occurred in recent years, as well as the rate of increase in the use of new technologies (AI, machine learning, accelerated underwriting, rating algorithms, etc.), and big data by insurers, the Working Group recommends that models 670 and 672 be amended to ensure that regulators can continue to provide consumer data privacy protections essential to meet the consumer data privacy challenges presented by the public use of technology and data by insurers in today's business environment.

The Working Group also recommends the NAIC's Market Regulation Handbook be updated, as necessary, to provide guidance to state insurance regulators so they can verify insurers' compliance the regulatory framework for consumer privacy protections.

Appendix A

National Association of Insurance Commissioners
Policy Statement on Consumer Data Privacy Protections

Because the business operations of insurance companies are dependent upon the collection and use of personal information and data, state insurance regulators have long understood the need to balance an insurance company's need to collect consumer information and data with the consumer's right to limit the collection and use of data.

The NAIC adopted the *Insurance Information and Privacy Protection Model Act* (Model #670) in 1980 to establish standards for the collection, use and disclosure of information gathered in connection with insurance transactions. A key aspect of this model is that it establishes a regulatory framework for consumers to (1) ascertain what information is being or has been collected about them in connection with insurance transactions; (2) obtain access to such information for the purpose of verifying or disputing its accuracy; (3) limit the disclosure of information collected in connection with insurance transactions; and (4) obtain the reasons for any adverse underwriting decision. This regulatory framework is facilitated through a requirement that insurers or agents provide a written notice to all applicants and policyholders regarding the insurer's information practices.

The NAIC adopted the *Privacy of Consumer Financial and Health Information Model Regulation* (Model #672) in 2000. The model regulation was drafted to implement the requirements set forth in Title V of the federal *Gramm-Leach-Bliley Act* (P.L. 106-102) of 1999 (GLBA). GLBA imposed privacy and security standards on financial institutions and directed state insurance commissioners to adopt certain data privacy and data security regulations. The model also contains provisions governing protection of health information that were taken directly from the Health Insurance Portability and Accountability Act Privacy Rule promulgated by HHS. The NAIC model regulation requires insurers to: (1) notify consumers about their privacy policies; (2) give consumers the opportunity to prohibit the sharing of their protected financial information with non-affiliated third parties; and (3) obtain affirmative consent from consumers before sharing protected health information with any other parties, affiliates, and non-affiliates. The key difference between the treatment of financial information and health information is that insurers must give consumers the right (with limited exceptions) to "opt out" of the disclosure or sharing of their financial information, but insurers must get explicit authorization ("opt in") before sharing health information.

This policy statement is based on the consumer protections set forth in these two models and serves the purpose of informing licensed insurance entities, consumers, and the other state and federal regulatory agencies on what the NAIC currently supports as the minimum consumer data privacy protections that are appropriate for the business of insurance. The policy statement is not intended to modify any existing NAIC models and does not carry the weight of law or impose any legal obligations in states that have adopted those models.

The policy statement addresses consumer data privacy protections of (1) transparency; (2) consumer control; (3) consumer access; (4) data accuracy; and (5) data ownership and portability. The policy statement intentionally excludes standards for data security and standards for the investigation and notification to an insurance commissioner of a licensed insurance entity's cybersecurity event, which are the subject of separate model laws and interpretive guidance.

The following definitions are used for the purposes of this policy statement.

A. "Adverse Decision" means declination of insurance coverage, termination of insurance coverage, charging a higher rate for insurance coverage, or denying a claim.
B. "Consumer" means an individual who is seeking to obtain, obtaining, or have obtained a product or service from

an insurer. For example, an individual who has submitted an application for insurance is a consumer of the company to which he or she has applied, as is an individual whose policy with the company has expired.

C. "Customer" means a consumer with whom an insurer has an on-going relationship.

D. "Licensee" means any insurer, producer, or other person licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to a state insurance law.

E. "Personal Information" means any individually identifiable information or data gathered in connection with an insurance transaction from which judgments can be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit, health, or any other personal characteristics. Personal information includes:

1. "Non-Public Personal Information," which means information that a consumer provides to a licensee to obtain an insurance product or service (like income, credit history, name and address); information about a consumer a licensee has as a result of a transaction involving an insurance product or service (like premium payment history, how much a life insurance policy is worth, and the value of personal property insured); and all other information about a consumer that a licensee uses in connection with providing a product or service to a consumer.
2. "Non-public personal health information," which means any information that identifies a consumer in some way, and includes information about a consumer's health, including past and present physical and mental health, details about health care, and payment for health care.

I. Transparency

A licensee should provide a clear and conspicuous notice to consumers that accurately reflects its privacy policies and practices when it first requests personal information about the consumer from the consumer or a third party.

A licensee should also provide a periodic notice of its privacy policies and practices to customers not less than annually during the continuation of the customer relationship.

If a licensee makes an adverse decision based on information/data that was not supplied by the consumer, the licensee should provide the consumer with the specific reasons for the adverse decision.

II. Consumer Control

Licensees should, at a minimum, provide consumers the opportunity to prohibit the sharing of their non-public personal information with third parties, except for specific purposes required or specifically permitted by law. (Opt-Out)

Licensees should obtain affirmative consent from consumers before sharing non-public personal health information with any other entity, including its affiliates and non-affiliates. (Opt-In)

III. Consumer Access

Any consumer should have the right to submit a request to a licensee to obtain access to his/her personal information used by the licensee in its operations. Upon request, the licensee should within 30 business days provide a copy of the consumer's personal information, an explanation on how the personal information was used (i.e., rating, underwriting, claims), and provide the source of the personal information. If personal information is in coded form, the licensee should provide an accurate translation in plain language.

IV. Data Accuracy

Within 30 business days after receiving a request from a consumer to correct, amend, or delete personal information used by the licensee in its operations, the licensee should either make the requested correction, amendment, or deletion or notify the consumer of its refusal to do so, the reasons for the refusal, and the consumer's right to file a statement of dispute setting forth what the consumer thinks is the correct information and the reasons for disagreeing with the licensee.

If the licensee corrects, amends, or deletes personal information, the licensee should notify any person or entity that has received the prior personal information within the last 7 years. If the licensee does not correct, amend, or delete the disputed personal information, the licensee should notify any person or entity that has received the prior personal information within the last 7 years of the consumer's statement of dispute.

V. Data Ownership and Portability

A customer should have the right to request a copy of his/her personal information that he/she has provided to the licensee for use in the licensee's operations. A licensee should provide a customer a copy of his/her personal information within 30 business days of the request. Examples of this type of personal information include telematics data and "Internet of Things" ("IoT") data.

Appendix B – Version 3

National Association of Insurance Commissioners
Resources on Consumer Data Privacy Protections
Reviewed by the Privacy Protections (D) Working Group

1. California Consumer Privacy Act (CCPA)
2. California Privacy Rights Act (CPRA)
3. Colorado Privacy Act (CPA)
4. General Data Protection Regulation (GDPR)
5. Health Insurance Portability and Accountability Act (HIPAA)
6. Gramm-Leach-Bliley Act (GLBA)
7. Federal Credit Reporting Act (FCRA)
8. NAIC Health Information Privacy Model Act #55
9. NAIC Insurance Data Security Model Act #668
10. NAIC Insurance Information and Privacy Protection Model Act #670
11. NAIC Privacy of Consumer Financial and Health Information Regulation #672
12. Virginia Consumer Data Protection Act (CDPA)
13. Troutman Analysis of Virginia Consumer Data Protection Act
14. Presentation by Dr. Karrol Kitt (The University of Texas at Austin) and Dr. Brenda J. Cude (University of Georgia) on the Additional Insurer Responsibility to Protect Consumer Data due to Consumers' Lack of Knowledge and Understanding of Privacy Risks
15. Presentation by Dr. Harold M. Ting (Consumer Healthcare Advocate) Exploring Results of His Secret Shopper Research and the Effects on the Privacy of Consumer Data
16. Nine Privacy Principles developed by Dr. Harold M. Ting (Consumer Healthcare Advocate)
17. Presentation by Clay McClure (Blue Cross Blue Shield Association) on the Need for Privacy Gap Analysis
18. Presentation by Damon Diedrich (CA) on California's Privacy Legislation (CCPA and CPRA)
19. Presentation by Katie Johnson (VA) on Virginia's Privacy Legislation
20. Abbreviated Data Privacy Legislation Chart 10.8.21 prepared by Jennifer McAdam (NAIC Legal)
21. State Privacy Law Comparison Chart 10.8.21 prepared by Jennifer McAdam (NAIC Legal)

22. Model #670 / CCPA Privacy Comparison prepared by Jennifer McAdam (NAIC Legal)
23. GLBA / HIPAA Privacy Comparison prepared by Jennifer McAdam (NAIC Legal)
24. 2021 NAIC Member Adopted Strategy for Consumer Privacy Protections provided by its parent committee, Market Regulation and Consumer Affairs (D) Committee, April 29, 2021
25. Privacy Briefing 2011.7.19 prepared by Jennifer McAdam and Lois Alexander
26. Final Exposure Draft Report to D Cmte on Privacy 11.18.21
27. First Working Group Exposure Draft of Privacy Policy Statement_082621.pdf
28. Comment Schedule for Draft Exposed 082621.pdf
29. MO670_041520_ExposureDraftTopics_with_042920_CommentsonSec1-9_rev082221.pdf
30. MO672_redline082221.pdf
31. Privacy Policy Statement Draft3 070121
32. Initial Privacy Policy Statement_Draft1_042821
33. ***MO670_041520_Exposure Draft Topics***
34. *Uniform Personal Data Protection Act*
35. Baker Donelson Summary of Privacy Laws
36. Article by Barbara Kiviat, Stanford University, "Which Data Fairly Differentiate? American Views on the Use of Personal Data in Two Market Settings." Sociological Science, published: January 13, 2021,

Summary:

In 2021, this working group had ten open calls between Mar. 29 and Nov. 22, 2021.

The Regulator-Only Subject Matter Experts had eight calls.

The Working Group heard eight presentations as well as Federal and State Legislative Updates at seven meetings in 2021:

1. Karrol Kitt (NAIC Consumer Representative)
2. Brenda Cude (NAIC Consumer Representative)
3. Harry Ting (NAIC Consumer Representative)
4. Clay McClure, BCBSA
5. Damon Diederich (CA)
6. Katie Johnson (VA)
7. Model #670 / CCPA Privacy Comparison by Jennifer McAdam (NAIC)
8. GLBA / HIPAA Privacy Comparison by Jennifer McAdam (NAIC)
9. Federal Legislative Updates at most open meetings by Brooke Stringer (NAIC)
10. State Legislative Updates at most open meetings by Jennifer McAdam (NAIC)
    a. Abbreviated Data Privacy Legislation Chart
    b. State Privacy Law Comparison Chart

Four NAIC Models were reviewed:

1. NAIC Health Information Privacy Model Act #55
2. NAIC Insurance Data Security Model Act #668
3. NAIC Insurance Information and Privacy Protection Model Act #670
4. NAIC Privacy of Consumer Financial and Health Information Regulation #672

State Laws reviewed:

1. California Consumer Privacy Act (CCPA)
2. California Privacy Rights Act (CPRA)
3. Colorado Privacy Act (CPA)
4. Virginia Consumer Data Protection Act (CDPA)

Federal Laws reviewed:

1. Health Insurance Portability and Accountability Act (HIPAA)
2. Gramm-Leach-Bliley Act (GLBA)
3. Federal Credit Reporting Act (FCRA)

Reviewed the European Union's General Data Protection Regulation (GDPR)

Drafts (All with Privacy Policy Statement in their titles) were exposed and posted for comment on:

1. April 28, 2021
2. July 1, 2021
3. August 26, 2021

The Final Exposure Draft Report (which included the Privacy Policy Statement as Appendix A) was exposed and posted for comment on November 18, 2021.