NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

Date: 3/23/21

Virtual Meeting
(in lieu of meeting at the 2021 Spring National Meeting)

PRIVACY PROTECTIONS (D) WORKING GROUP
Monday, March 29, 2021
4:00 – 5:00 p.m. ET / 3:00 – 4:00 p.m. CT / 2:00 – 3:00 p.m. MT / 1:00 – 2:00 p.m. PT

ROLL CALL

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

NAIC Support Staff: Lois E. Alexander

AGENDA

1. Consider Adoption of its 2020 Fall National Meeting Minutes — Attachment A
   —*Cynthia Amann (MO)*

2. Receive Status Reports—*Cynthia Amann (MO)*
   a. Federal Privacy Legislation—*Brooke Stringer (NAIC)*
   b. State Privacy Legislation—*Jennifer McAdam (NAIC)* — Attachments B and C

3. Review the 2021 NAIC Member-Adopted Strategy for Consumer Data Privacy Protections—*Cynthia Amann (MO)* — Attachment D

4. Discuss Comments Received on 2020 Fall National Meeting Verbal Gap Analysis
   a. American Council of Life Insurers (ACLI) —Robert Neill (ACLI) — Attachment E
   b. Coalition of Health Carriers—Chris Petersen (Arbor Strategies LLC) — Attachment F
   c. National Association of Mutual Insurance Companies (NAMIC) — Attachment G
      —*Cate Paolino (NAMIC)*
   d. American Property Casualty Insurance Association (APCIA) — Attachment H
      —*Angela Gleason (APCIA)*

5. Announce the Consumer Privacy Protections Panel at the NAIC Virtual Insurance Summit, June 14–21, 2021—*Cynthia Amann (MO)*

6. Discuss Any Other Matters Brought Before the Working Group—*Cynthia Amann (MO)*

7. Adjournment

W:\National Meetings\2021\Spring\Cmte\D\Privacy Protections\PPWG Agenda Interim Mtg Spring 21.Docx

Draft: 12/1/20

Privacy Protections (D) Working Group
Virtual Meeting (*in lieu of meeting at the 2020 Fall National Meeting*)
November 20, 2020

The Privacy Protections (D) Working Group of the Market Regulation and Consumer Affairs (D) Committee met Nov. 20, 2020. The following Working Group members participated: Cynthia Amann, Chair, and Marjorie Thompson (MO); Ron Kreiter, Vice Chair (OK); Damon Diederich (CA); Erica Weyhenmeyer (IL); LeAnn Crow (KS); T.J. Patton (MN); Raven Collins (OR); Gary Jones (PA); and Katie C. Johnson (VA). Also participating were Vanessa Darrah (AZ); Scott Woods (FL); and John Haworth (WA).

1. Adopted its July 30 Minutes

Ms. Amann said the Working Group met July 30 and took the following action: 1) adopted its May 5 minutes; 2) heard a presentation that included a comparative analysis and comments received July 24 by the Blue Cross Blue Shield Association (BCBSA) and the Health Coalition; and 3) made plans to begin a gap analysis discussion by Working Group members, interested state insurance regulators, and interested parties using the *Privacy of Consumer Financial and Health Information Regulation* (#672) as a baseline model.

Mr. Kreiter made a motion, seconded by Ms. Weyhenmeyer, to adopt the Working Group's July 30 minutes (*see NAIC Proceedings – Summer 2020, Market Regulation and Consumer Affairs (D) Committee, Attachment Five*). The motion passed unanimously.

2. Discussed Initial Draft Gap Analysis of Consumer Issues

Ms. Amann said the next item on the agenda is to discuss the initial draft gap analysis of consumer issues, and she asked Lois E. Alexander (NAIC) to provide a reminder of what brought the Working Group to this point.

Ms. Alexander said the Working Group kicked off its task during the 2019 Fall National Meeting in Austin, TX by providing a draft discussion document in the form of a workplan that included a privacy briefing. She said this workplan also provided a schedule and overviews of the *NAIC Insurance Information and Privacy Protection Model Act* (#670), Model #672, the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and State Data Privacy Legislation. She said the Working Group met in February to discuss next steps and receive updates from Brooke Stringer (NAIC) on federal legislation and Jennifer McAdam (NAIC) on state legislation, including privacy charts comparing the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accessibility Act of 1996 (HIPAA), the CCPA and Model #670, and detailed and abbreviated data privacy charts of state legislation. Progress by the Working Group continued during the pandemic, but at a slower pace than was anticipated in the schedule. Ms. Alexander said next steps include a draft revision of Model #670 from the subject matter expert (SME) state insurance regulator group that was exposed for comment in April, with comments being discussed during the May meeting. Comments presented at the May meeting indicated that revisions to Model #670 would not be the best approach going forward. Ms. Alexander said the July meeting began with a presentation that included a comparative analysis using Model #672 by the BCBSA and Arbor Strategies LLC on behalf of the Health Coalition, and it ended with the Working Group reviewing plans to begin a gap analysis discussion using Model #672 as a baseline model.

Ms. Amann said as a reminder, the Working Group's 2020 charges are 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 certain NAIC models, such as the *NAIC Insurance Information and Privacy Protection Model Act* (#670) and the *Privacy of Consumer Financial and Health Information Regulation* (#672), by the 2020 Summer National Meeting.

Ms. Amann said during the Working Group's last meeting, it determined that it would separate its gap analysis discussions into three parts: Consumer Issues, Industry Obligations and Regulatory Enforcement. She said it was also determined that, where appropriate, the NAIC Data Guiding Principles would be applied and definitions would be updated to align with those already discussed and adopted by other NAIC groups working on similar issues, such as the Artificial Intelligence (EX) Working Group, the Big Data (EX) Working Group, the Accelerated Underwriting (A) Working Group, etc. However, she said today's focus will be on the following consumer issues: notifications, portability, opt-ins/opt-outs and disclosures.

Ms. Amann said the first issue is consumer notifications. She said using the workplan from last fall, the Working Group will compare the consumer notification requirements in Section V—State Privacy Legislation to the consumer notification requirements in Section II—Model #672. She said State Privacy Legislation requires privacy notice to consumers. She said Article II—Privacy and Opt Out Notices for Financial Information of Model #672, which begins on page 672-15, has detailed requirements for insurers to follow regarding the type, method and timing of initial, annual and revised privacy notices to consumers about its privacy policies and practices; so at first review, it appears there is no gap. However, the Working Group would like to discuss the following questions: 1) how consumer notifications are handled currently; 2) whether this method is still effective or there are gaps that require revision; and 3) what areas revisions are needed and why if there are gaps.

Chris Petersen (Arbor Strategies LLC) said the consumer notification and disclosure requirements in the GLBA and HIPAA are very comprehensive and based on set timeframes at initial point of sale and annually thereafter. As a result, he said consumers believe that they get too many notices causing consumers to ignore or toss the notices without being read, so this type of requirement is ineffective. He said federal laws might get in the way of this Working Group taking action that could help consumers, like triggering notices on occurrences rather than on timing. He said encouraging consumers to opt-in to electronic versions would also be very productive. He said the sample provisions in the GLBA are prescribed by law.

Ms. Johnson said when Virginia added the elements of the GLBA to its code, the required notices for insurance were removed from the combined notices and put into security under the *Insurance Data Security Model Law* (#668). She said the General Assembly would not mandate the use of electronic notices because many consumers do not have computer access, so opt-in is required instead. She said companies wanted to post rather than mail the notices. She said Virginia allows posting of the notices, but it also requires companies to provide paper copies to consumers free of charge. Ms. Amann said she receives paper notices from several companies that she throws away without reading. She said her preference is a notice on her billing statement of a web notice via link because it is so easy. Ms. Johnson asked if the GLBA has any restrictions to prevent states and companies from doing this type of notice. Ms. Johnson said the abbreviated notice provided by the federal government in 2015 requires states and companies to follow it exactly or risk the federal government taking this responsibility from state jurisdiction. Ms. Darrah said Arizona requires that a script and recording be available online for the hearing impaired. Mr. Petersen said it could not be required, but it could be offered as an option. Mr. Haworth said accessibility standards require the ability to listen as well as read. Ms. Amann said the assignment going forward is to receive comments prior to the next meeting and consider any option submitted if it helps to streamline and get notices into a consumer's hands.

Ms. Amann said the second issue is consumer portability. In Section V of the workplan, she said State Privacy Legislation includes a consumer right of a portable data format; and in Section II of the workplan, Article II and Article V—Rules for Health Information of Model #672, which begins on page 672-30, provide methods for individuals to prevent a licensee from disclosing that information; i.e., "opt out" for financial info and "opt in" for health information, so it appears there is no gap. However, the Working Group would like to discuss the following questions: 1) how consumer notifications are handled currently; 2) whether this method is still effective or there are gaps that require revision; and 3) what areas revisions are needed and why if there are gaps. Ms. Amann asked for comments to be submitted about portability as well.

Ms. Amann said the third issue is consumer opt-ins versus opt-outs. She said in the workplan, Section V. State Privacy Legislation requires a consumer opt-in or opt-out standard. However, in Article II of Model #672 provides "opt out" for financial info, and Article V of Model #672 provides "opt in" for health information. Ms. Amann said in this case, it appears that there is a gap that will need to be addressed with these and other questions: 1) how consumer notifications are handled currently; 2) whether this method is still effective or there are gaps that require revision; and 3) what areas revisions are needed and why if there are gaps. She said at issue here is whether the consumer fully understands what their choice to opt-in or opt-out really means about control over their data within the insurance industry. Ms. Johnson said Virginia kept the whole list of opt-ins and opt-outs from the GLBA in its legislation that would have to be untangled if Virginia was to pursue a different option at this point. Ms. Amann said any other options would have to work within the GDPR and the CCPA as well. She said the question is really if any provision is still needed that could help to improve business practices and consumer protections. Mr. Petersen asked that the Working Group be mindful that anything it does be for all businesses, not just for the insurance industry, so as not to disadvantage the insurance industry or any other business concern. Ms. Amann agreed and said this issue needs more discussion.

Ms. Amann said the fourth issue is consumer disclosures. She said in the workplan, Section V. State Privacy Legislation includes: 1) a requirement to disclose information collected; 2) a requirement to disclose shared information; 3) a requirement to disclose sources of information; 4) a requirement to disclosure business purpose; and 5) a requirement to disclosure third party involvement. However, she said in Article III—Limits on Disclosures of Financial Information, which begins on page 672-15, and Article V of Model #672 describe the conditions under which a licensee may disclose nonpublic personal health information and nonpublic personal financial information about individuals to affiliates and nonaffiliated third parties. Ms.

Amann said Model #672 appears to cover this requirement in general, but not specifically, so there may be a gap. For each of these requirements, she said the Working Group would like to address the following questions: 1) how consumer notifications are handled currently; 2) whether this method is still effective or there are gaps that require revision; and 3) what areas revisions are needed and why if there are gaps. Ms. Amann said artificial intelligence (AI), accelerated underwriting, and other big data advancements are being developed faster than consumers can tell what is happening. She said the Accelerated Underwriting (A) Working Group is in discussions now. She said third party involvement needs to be addressed, as well as when and how consumers can become involved. She said in this regard, Model #672 needs to be updated. Mr. Haworth asked how the data from driving a car would be used if a consumer uses their cell phone to buy the car, but they are not the person who will be driving the car. He also asked how the consumer would know who, how and why the data on driving that car is being used. Birny Birnbaum (Center for Economic Justice—CEJ) said one cannot separate disclosure from consent. He asked how a consumer knows to what uses their consent is being given. He said general consent should not be allowed because it does not tell consumers any real information about where or for what their consent is being used. He also said it does not tell consumers what data they have control over—i.e., driving record— or who owns the data—i.e., the insurance company, the car dealership, or the consumer. He said this also relates to portability, as a consumer cannot control the sending of data to another carrier or affiliate. Ms. Amann said keeping track of and keeping up with new technology cannot control what consumers read and know either. She said there is a need to review the content of the notices and a consumer's understanding over who has control over their data. Mr. Petersen said the Working Group should proceed with caution because it is hard to separate consumers from business and regulation. He said in the end, it would be necessary to see how all four issues are interconnected and what interplay there is between them.

Ms. Amann said the Working Group will collect comments about consumer issues for the next few weeks and the Working Group will have a series of regulator-only calls during this time in order to provide a completed outline of the insurance functions of Model #672 before Christmas with an email in early January 2020 exposing it for comments. Mr. Kreiter asked that comments be included for all three areas, not just for consumer issues.

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

W:\National Meetings\2020\Fall\Cmte\D\Privacy Protections\Privacyprot_11min.Docx

In	Opt-in
Out*	Opt-out in certain instances
B	Opt-in or Opt-out
CP	Office of Consumer Protection
CA	Director of the Division of Consumer Affairs in the Department of Law and Public Safety
SD	Secretary of the Department of Consumer Affairs
X+	Attorney General, County District Attorney, or City Corporation General
S	Private rights of action for security violation only
P	Partial exemption only. Still subject to private action.

State	Citation / Status	Disclose Collected Info	Disclose Sources of info	Disclose Business Purpose	Disclose Third Party Involvement	Right to Delete Information	Portable Format	Right to Correct Information	Right to Restrict Use	Opt-Out/Opt-In	Private Right of Action	Enforced by AG	Anti-Discrimination	HIPAA Exemption	GLBA Exemption	Other Exemption	Establishes a Committee
PASSED BILLS																	
California	**CAL. CIV. CODE §§ 1798.100-199 (2020)**	**X**	**X**	**X**	**X**	**X**	**X**			**Out***	**S**	**X**	**X**	**X**	**P**	**P**	
California	**AB713/In committee/Amendment[1]**															X	
California	**AB 2751/In Committee/Amendment[2]**																
California	**§999.306/Amendment[3]**																
Hawaii	**HCR 225: 4/3/2019 Adopted**																**X**
Louisiana	**HR 249 / Adopted**																**X**
Maine	**ME. REV. STAT. tit. 35-A, § 94 (2019)[4]**									**In**							
Nevada	**NEV. REV. STAT. ANN. § 603A.300 (2019)**	**X**								**Out**	**X**			**X**	**X**	**X**	
North Dakota	**HB 1485 / Adopted**																**X**
Texas	**HB 4390 / Adopted**																**X**
Virginia	**SB 1392/Adopted**	**X**		**X**	**X**	**X**	**X**	**X**		**Out**			**X**	**X**	**X**	**X**	**X**
ACTIVE BILLS																	
Alabama	HB 2: READ 2/2/2021, in committee	X	X			X	X			Out	X		X	X	X		
Arizona	HB 2865/Intro 2/15/21	X		X		X	X	X	X			X		X	X		
Colorado	SB21-190/Intro 3/19/21	X		X		X	X	X		Out		X		X	X	X	
Connecticut	SB 893/Referred to committee					X		X		Out		X		X		X	
Connecticut	SB 156/ Public hearing	X								Out	X						
Florida	HB 969/In subcommittee	X				X	X	X		Out			X				
Florida	SB 1734/Introduced 3/10/2021	X				X		X	X	Out	X		X	X	X		
Illinois	HB 3910/In committee		X	X	X	X	X			Out*	X	X	X	X	X	X	
Kentucky	HB 408/Referred to committee	X		X		X				Out		X	X	X		X	

[1]Amendment to existing CCPA that exempts information collected for biomedical research.
[2] Amendment to existing CCPA that revises definition of "deidentified"; cannot be used to infer other information about/linked to a consumer; business must take "reasonable measures".
[3] Amendments to existing CCPA that changes opt-out (offline collections & notices, opt-out icon, make opt-out requests easy to submit); authorized agents may need to submit proof that consumer gave them permission to submit request.
[4] Only applies to internet service providers.

In	Opt-in
Out*	Opt-out in certain instances
B	Opt-in or Opt-out
CP	Office of Consumer Protection
CA	Director of the Division of Consumer Affairs in the Department of Law and Public Safety
SD	Secretary of the Department of Consumer Affairs
X+	Attorney General, County District Attorney, or City Corporation General
S	Private rights of action for security violation only
P	Partial exemption only. Still subject to private action.

State	Citation / Status	Disclose Collected Info	Disclose Sources of info	Disclose Business Purpose	Disclose Third Party Involvement	Right to Delete Information	Portable Format	Right to Correct Information	Right to Restrict Use	Opt-Out/Opt-In	Private Right of Action	Enforced by AG	Anti-Discrimination	HIPAA Exemption	GLBA Exemption	Other Exemption	Establishes a Committee
ACTIVE BILLS (cont.)																	
Maryland	SB 0930/First reading	X		X	X	X	X			Out		X	X	X	X	X	X
Massachusetts	SD 1726	X		X	X	X	X	X		In	X			X			
Minnesota	HB 1492/Referred to Committee	X		X	X	X	X	X		Out		X	X	X	X	X	
New Jersey	A5448 / In Committee	X			X			X		Out		CA	X	X	X	X	X
New Jersey	A3283 / In Committee	X		X	X	X	X	X	X	In		X*		X	X	X	
New Jersey	A3255 / In Committee	X			X	X	X			In	X		X	X	X	X	
New York	A400/S1349 / In Committee	X			X						X	X					
New York	A3818/ S1570 In Committee[5]	X	X	X	X	X						X	X				
New York	A680/In committee	X		X	X	X	X	X	X	Out	X	X		X	X		
New York	SB567/In committee	X	X	X	X					Out	X	X	X	X		X	
New York	A405/In committee[6]									Out		X					
New York	A674/In committee[7]				X					In	X		X				
Oklahoma	HB 1602/In Senate	X	X	X	X	X		X		Out		X	X	X	X	X	
Oklahoma	HB 1130/In committee	X	X	X	X			X				X					
Washington	HB 1433/Introduced 1/2/2021	X				X	X	X			X	X	X	X			
Washington	SB 5062/In committee					X	X	X		Out		X	X	X	X	X	

[5] Only applies to government entities and contractors.
[6] Only applies to advertising networks.
[7] Only applies to internet service providers.

Proposed State Privacy Laws Comparison Chart

Alabama Consumer Privacy Act Bill HB 216	
Status	Read 2/2/21, in committee
Looks Like	Modified CCPA
Scope	For profit entities doing business in AL and processing AL resident personal information
Rights	Access, know, deletion, not be discriminated against, data portability
Opt In/Out	Opt-out of sales
Enforcement	Violation of act is a violation of state Deceptive Trade Practices Act. Private right of action for data breaches
Exemptions	GLBA information; HIPAA information

Arizona, Article 5. Data and Security Standards Bill HB 2865	
Status	Introduced 2/15/21
Looks Like	GDPR/CCPA mash-up
Scope	$25M + controls/processes personal data of 100,000 state residents or is a data broker
Rights	Confirm processing/sales to **data brokers**, access, correction, deletion, restrict and object to processing, data portability
Opt In/Out	
Enforcement	Attorney General
Exemptions	GLBA info, HIPAA info

Colorado SB21-190	
Status	Introduced 3/19/21
Looks Like	VDCPA, WPA
Scope	Controllers that conduct business in Colorado or produce products or services that are intentionally targeted to residents of Colorado and that (1) control or process the personal data of 100,000 or more consumers during a calendar year and/or (2) derive revenue or receive a discount on the price of goods or services from the "sale" of personal data and process or control the personal data of 25,000 or more consumers.
Rights	Delete, correct, portable format
Opt In/Out	Opt out of the processing of ALL personal data concerning the consumer. Consent to processing of sensitive data.
Enforcement	AG
Exemptions	Data & entity GLBA, HIPAA, other

Proposed State Privacy Laws Comparison Chart

Connecticut Bill SB 893	
Status	Introduced 2/17/21, Referred to committee
Looks Like	
Scope	Persons that conduct business in this state or persons that produce products or services that are targeted to residents of this state and that: (1) During a calendar year, control or process personal data of not less than one hundred thousand consumers, or (2) control or process personal data of not less than twenty-five thousand consumers and that derive more than fifty per cent of their gross revenue from the sale of personal data.
Rights	Right to access, correct, delete and obtain a copy of personal data.
Opt In/Out	opt out of the processing of personal data for the purposes of targeted advertising.
Enforcement	Attorney General
Exemptions	HIPAA, non-profits, higher education

Connecticut "An Act Concerning Consumer Privacy" Bill S.B. No. 156	
Status	Introduced 1/2021; public hearing 2/25
Looks Like	
Scope	
Rights	(1) require businesses to 2 disclose the proposed use of any personal information, (2) give consumers the right to discover what personal information such business possesses and to opt out of the sale of such information
Opt In/Out	
Enforcement	Cause of action and penalties for violations of such requirements
Exemptions	

Florida Consumer Data Privacy Bill HB 969	
Status	In Subcommittee
Looks Like	Sweeping

Proposed State Privacy Laws Comparison Chart

Scope	For profit businesses in state that either: have global annual gross revenues in excess of $25 million; annually buys, sells, or shares for commercial purposes the personal info of 50,000 or more consumers; or derives 50% or more of its global revenues from selling or sharing personal info.
Rights	Disclose, delete, correct
Opt In/Out	Opt-out; Opt-out of 3rd party disclosure
Enforcement	Private right of action; Dept. of Legal Affairs
Exemptions	
Other	Right to Opt-in for those under 16

Proposed State Privacy Laws Comparison Chart

Florida Privacy Protection Act Bill SB 1734	
Status	Introduced 3/10/2021
Looks Like	Sweeping
Scope	For profit businesses in state that either: have global annual gross revenues in excess of $25 million; annually buys, sells, or shares for commercial purposes the personal info of 50,000 or more consumers; or derives 50% or more of its global revenues from selling or sharing personal info.
Rights	Right to request certain data be disclosed, deleted or corrected. Direct certain businesses not to sell personal info
Opt In/Out	Opt-in or opt-out of sale or sharing of such data
Enforcement	Private Right of action; Dept. of Legal Affairs
Exemptions	HIPAA, GLBA
Other	Can't sell info if business has actual knowledge that consumer is younger than 16 years old

Illinois Consumer Privacy Act Bill HB 3910	
Status	Assigned to Civil Committee
Looks Like	Disclosure-focused
Scope	Annual gross revenues in excess of $25 million; or buys, receives, sells or shares personal info of 50,000 or more consumers, households, or devices; or derives 50% or more of its annual revenues from selling consumers' personal info
Rights	Right to request disclosure, deletion with some exceptions
Opt In/Out	Opt-out of sale to third parties. Opt-in for those under 16.
Enforcement	Civil action; AG
Exemptions	HIPAA, GLBA, Driver's Privacy Protection Act
Other	Provide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information"

Proposed State Privacy Laws Comparison Chart

Kentucky Bill HB 408	
Status	Referred to Committee
Looks Like	
Scope	Annual gross revenues in excess of $25 million; or buys, receives, sells or shares personal info of 50,000 or more consumers, households, or devices; or derives 50% or more of its annual revenues from selling consumers' personal info
Rights	Right to request changes to personal info
Opt In/Out	Opt-out of sale of personal info. Opt-in under 16
Enforcement	AG
Exemptions	HIPAA entities; motor vehicle
Other	Provide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information"

Maryland Consumer Personal Information Privacy Bill SB 9030	
Status	First reading
Looks Like	
Scope	Annual gross revenues in excess of $25 million; or buys, receives, sells or shares personal info of 100,000 or more consumers, households, or devices; or derives 50% or more of its annual revenues from selling consumers' personal info
Rights	Delete.
Opt In/Out	Opt-out of third-party disclosure. May not disclose to third-party if consumer is under 16.
Enforcement	AG may adopt regulations. Violation is an unfair, abusive, or deceptive trade practice w/in meaning of Title 13.
Exemptions	HIPAA, GLBA, others
Other	

Proposed State Privacy Laws Comparison Chart

Massachusetts Information Privacy Act Bill SD 1726	
Status	
Looks Like	
Scope	
Rights	Know, access, correction, data portability, and deletion. Individuals 13 and older deemed competent to exercise all rights.
Opt In/Out	Opt-in. A covered entity must obtain consent.
Enforcement	Private right of action. Mass. Information privacy commission
Exemptions	HIPAA
Other	Prohibition of surreptitious surveillance

Minnesota Consumer Data Privacy Act Bill HB 1492	
Status	Intro 2/22/21, referred to Committee
Looks Like	
Scope	Minn. Business that during a calendar year controls or processes personal data of 100,000 consumers or more; or derives over 25% of gross revenue from the sale of personal data and processes or controls personal data of 25,000 consumers or more.
Rights	Correct, delete, obtain in portable format
Opt In/Out	Opt-out of processing of personal data for targeted advertising, sale, or profiling. Opt-in for children and for sensitive personal data.
Enforcement	AG
Exemptions	HIPAA, GBLA, Driver's Privacy Protection Act, others
Other	

Proposed State Privacy Laws Comparison Chart

New Jersey Bill AB 5448	
Status	In committee
Looks Like	
Scope	commercial Internet websites and online services
Rights	Right to make changes
Opt In/Out	Opt-out
Enforcement	AG
Exemptions	HIPAA, GLBA, other
Other	
New Jersey Disclosure and Accountability Transparency Act	
Bill	A3283
Status	In committee
Looks Like	
Scope	
Rights	Deletion, correction, or restriction of information. Object to disclosure to a third party.
Opt In/Out	Opt-in
Enforcement	Office of Data Protection and AG
Exemptions	HIPAA, GLBA, DPPA, FCRA
Other	Established the Office of Data Protection and Responsible Use. Processing sensitive personal info prohibited. In event of data breach, controller has 72 hrs to notify office.

New Jersey Bill A3255	
Status	In committee
Looks Like	
Scope	Annual gross revenues in excess of $25 million; or buys, receives, sells or shares personal info of 50,000 or more consumers, households, or devices; or derives 50% or more of its annual revenues from selling consumers' personal info
Rights	Deletion, portable format
Opt In/Out	Opt-in
Enforcement	AG
Exemptions	HIPAA, GLBA, DPPA, FCRA
Other	

Proposed State Privacy Laws Comparison Chart

New York "The Right to Know Act of 2021" Bill A400/S1349 (older versions of bill in previous years)	
Status	In committee
Looks Like	
Scope	
Rights	
Opt In/Out	
Enforcement	Private right of action or brought by AG, DA, city attorney
Exemptions	
Other	Restricts the disclosure of personal information by businesses

New York Bill A3818/ S1570	
Status	In committee
Looks Like	
Scope	Only applies to government entities and contractors.
Rights	Disclosure, deletion
Opt In/Out	
Enforcement	AG for guidance
Exemptions	FCRA
Other	

New York Privacy Act Bill A680	
Status	In committee
Looks Like	
Scope	
Rights	Delete, correct, restriction
Opt In/Out	Opt-in or out to data processing. Opt-in to third party transfers
Enforcement	Private right of action, AG
Exemptions	HIPAA, GLBA
Other	

Proposed State Privacy Laws Comparison Chart

New York Bill SB567	
Status	In committee
Looks Like	
Scope	Annual gross revenues in excess of $50 million; or sells or shares personal info of 100,000 or more consumers, households, or devices; or derives 50% or more of its annual revenues from selling consumers' personal info
Rights	Disclosure
Opt In/Out	Opt-out. Under 16, opt-in
Enforcement	Private right of action; AG
Exemptions	HIPAA, FCRA
Other	"Do Not Sell Personal Information" link on webpage

New York Online Consumer Protection Act Bill A405	
Status	In committee
Looks Like	
Scope	Advertising network: company that is collecting online consume activity for the purpose of ad delivery
Rights	
Opt In/Out	Opt-out
Enforcement	AG
Exemptions	
Other	

New York Bill A674	
Status	In committee
Looks Like	
Scope	Internet Service Provider
Rights	
Opt In/Out	Opt-in
Enforcement	Private right of action
Exemptions	
Other	Prohibits the disclosure of personally identifiable information by an internet service provider without the express written approval of the consumer.

Proposed State Privacy Laws Comparison Chart

Oklahoma Computer Data Privacy Act Bill 1602	
Status	In senate
Looks Like	
Scope	Gross revenue in excess of $10 million; or buys, sells, receives, r shares for commercial purposes the personal info of 50,000 or more consumers; or derives 25% annual revenue from selling consumers' personal info
Rights	Delete, correct
Opt In/Out	Out
Enforcement	AG
Exemptions	HIPAA, GLBA, other
Other	

Oklahoma Bill HB 1130	
Status	In committee
Looks Like	
Scope	
Rights	Request changes
Opt In/Out	
Enforcement	AG
Exemptions	
Other	

Proposed State Privacy Laws Comparison Chart

Virginia Consumer Data Protection Act Bill SB 1392 (identical to HB 2307)	
Status	Adopted; Effective date: 1/1/2023
Looks Like	GDPR, CCPA, CPRA. More business friendly than CA
Scope	Applies to all persons that conduct business in the Commonwealth and either (i) control or process personal data of at least 100,000 consumers or (ii) derive over 50 percent of gross revenue from the sale of personal data and control or process personal data of at least 25,000 consumers.
Rights	rights to access, correct, delete, obtain a copy of personal data
Opt In/Out	opt out of the processing of personal data for the purposes of targeted advertising
Enforcement	AG has exclusive authority to enforce
Exemptions	GLBA, HIPAA, nonprofits, higher education, government
Other	Directs Joint Commission to establish group to review act and issues related to its implementation. Consent for collection of sensitive personal info.

Washington People's Privacy Act Bill HB 1433	
Status	Introduced 1/2/2021
Looks Like	
Scope	"Covered entity" means a person or legal entity that is not a governmental entity and that conducts business in Washington state, processes captured personal information, and (a) has earned or received $10,000,000 or more of annual revenue through 300 or more transactions or (b) processes and/or maintains the captured personal information of 1,000 or more unique individuals during the course of a year.
Rights	Delete, correct, not be subject to surreptitious surveillance
Opt In/Out	Opt-in
Enforcement	Private right of action; AG
Exemptions	HIPAA
Other	

Proposed State Privacy Laws Comparison Chart

Washington Privacy Act of 2021 Bill SB 5062	
Status	In committee
Looks Like	
Scope	Business in WA that either: during a calendar year, controls or processes personal data of 100,000 consumer or more; or Derives over 25% of gross revenue from the sale of personal data and processes or controls personal data of 25,000 consumers or more
Rights	Correct, delete
Opt In/Out	Opt-out
Enforcement	AG
Exemptions	HIPAA, FCRA, GLBA
Other	

NAIC Member Adopted Strategy for Consumer Data Privacy Protections

1. Charge the Market Regulation and Consumer Affairs (D) Committee with:
    a. Summarizing consumer data privacy protections found in existing NAIC models – *Health Information Privacy Model Act (Model #55), Insurance Information and Privacy Protection Model Act (Model #670), Privacy of Consumer Financial and Health Information Regulation (Model #672)*.
    b. Identifying notice requirements of states, the European Union's General Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA) and how insurers may be subject to these requirements.
    c. Identifying corresponding consumer rights that attach to notice requirements, such as the right to opt-out of data sharing, the right to correct or delete information, the right of data portability, and the right to restrict the use of data and how insurers may be subject to these requirements.
    d. Setting forth a policy statement on the minimum consumer data privacy protections that are appropriate for the business of insurance.
    e. Delivering report on items (a. – d.) above by NAIC fall national meeting.
2. Engage with state attorneys general (AGs), Congress, and federal regulatory agencies on state and federal data privacy laws to minimize preemption provisions and maximize state insurance regulatory authority.
3. Reappoint the Privacy Protections (D) Working Group to revise NAIC models, as necessary, to incorporate minimum consumer data privacy protections that are appropriate for the business of insurance. Complete by NAIC fall national meeting.

ACLI
Financial Security for Life

Kate Kiernan
Vice President & Deputy, Policy Development

December 21, 2020

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 soliciting stakeholder comments on your ongoing review of past and current consumer privacy frameworks. The American Council of Life Insurers respectfully submits the following comments on your recent request for input.

Amid technological transformation, consumers and businesses need privacy standards that clearly delineate the appropriate collection, use and sharing of personal information. While modernization of existing privacy laws is arguably necessary, we believe we should avoid creation of a system which would provide additional complexity such as differing consumer rights, varying levels of protections, fragmented implementation, and legal uncertainty. These are the unfortunate circumstances consumers and businesses are facing in California.

As we mentioned in our previous comment letters, the insurance industry is a consumer privacy leader in adhering to clear obligations in the appropriate collection, use and sharing of personal information. Our industry has appropriately managed consumers' confidential medical and financial information for decades and, in some instances, over a century. Fittingly, insurers have been subject to comprehensive federal and state privacy laws and regulations. These laws have reflected an essential balance between consumers' valid privacy concerns and the proper use of personal information by companies to the benefit of existing and prospective customers.

We believe it is important for insurance regulators to distinguish our industry from other businesses in the data driven technology sector. Insurers collect personal information for risk assessment purposes in order to provide consumers with options from which they may select products to fit their unique individual needs. Consumers derive benefit from the information they provide to insurers in many ways, such as, fairly assessing risk and guarding against fraud, while insurers are able to develop pricing that correlates to the risk. Consumers have an expectation, when they request

American Council of Life Insurers | 101 Constitution Ave, NW, Suite 700 | Washington, DC 20001-2133
(202) 624-2463 t | katekiernan@acli.com

products from insurers, that insurers collect this information with the consumer's consent in order to provide the products or services that they have requested or have shown an interest in. As we will discuss further in our comments below, insurers provide transparent notice regarding the collection and use of personal information in the course of business under both state and federal regulatory requirements.

We offer the following thoughts to the specific areas on which the Privacy Protections Working Group requested comment, including notice, portability, opt-in, opt-out, and disclosure.

Consumer Notice

We support the proposition that consumers should have easily accessible and transparent notice regarding information collected about them, the purposes for which it will be used, and how it will be protected. We believe that notice should be clear and conspicuous, and simple to understand. While a uniform federal approach to data privacy would best serve consumers and companies, the 2021 Washington Privacy Act proposed draft currently provides the most balanced and thoughtful approach being considered at the state level. Through the course of a multi-year debate, numerous stakeholders have had input into the proposal, every aspect of which has been thoroughly vetted. The Washington Privacy Act combines strong consumer privacy protections with flexibility for company compliance. In particular, the notice provisions are clear and concise without overly prescriptive complexity, such as we have seen in California and other proposals. The Washington State consumer notice provision is an example of well-balanced clarity:

(a) Controllers shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:
  (i.) The categories of personal data processed by the controller;
  (ii.) The purposes for which the categories of personal data are processed;
  (iii.) How and where consumers may exercise the rights contained in [consumer rights delineation section] of this act, including how a consumer may appeal a controller's action with regard to the consumer's request;
  (iv.) The categories of personal data that the controller shares with third parties;
  (v.) The categories of third parties, if any, with whom the comptroller shares personal data.
(b) If a controller sells personal data to third parties or processes personal data for targeted advertising, it must clearly and conspicuously disclose such processing, as well as the manner in which a consumer may exercise the right to opt out of such processing, in a clear and conspicuous manner.

And while focusing on consumer privacy notice, the Working Group should continue to explore simplification of the current notice process and seek to eliminate current and future duplication of notice and delivery. As the Working Group has discussed, consumers arguably receive too many complex privacy notices which results in little value to consumers. To align with modern privacy frameworks such as in Canada, Europe and Asia, policymakers should strive to reduce the number of notices while making the content understandable to the average person, relevant to their situation, and ensure that consumers are informed when material changes to privacy practices involving their personal information occur. For instance, using the same method that is used to collect personal information to deliver the privacy notice gives the consumer contextual background for the contents of the notice. One example of modernization in this area is the concept of "just-in-time" notices. Just-in-time privacy notices give consumers the information they need to know at the time personal information is collected, or a decision about their personal information is being made. Pop-up boxes or a hyperlink in an online form which provides relevant information to a consumer as they fill out the form are examples. And notice provided by text message, on a website, on a mobile app, or by

email, are all additional examples of how relevant and meaningful notice can be provided to consumers.

Portability

Data portability is generally regarded as the ability to allow individuals to obtain and reuse their own personal information across different services in a commonly used and machine-readable format. It is highly relevant in health care, with fitness devices, and in the social media context where an individual may wish to move their photos, activity data and other content in a convenient manner from one platform to another. Apart from health coverage portability, which provides people the ability to transfer their health coverage from one provider to another when changing jobs, demand by consumers for data portability is far less prevalent in the insurance world. This is mainly due to the fact that most insurance products are underwritten, different insurers often have different acceptance criteria, and consumers mostly turn to the original source of the information, such as a health care provider, for a current copy of the personal information they wish to share with another entity or platform.

Very low volumes of requests have been experienced by insurers under HIPAA's *Right to Access Protected Health Information*. In Europe, the concept of data portability introduced by Article 20 of the GDPR is limited to that which consumers have previously provided, includes direct transfers to another data controller if technically feasible, and only applies to automatic processing when personal data is being processed under the lawful basis of consent or performance of a contract. We know of little to no demand in the U.S. or Europe from consumers for portability in the life insurance context, nor of any requests from customers to ask their insurer to transfer the customers' personal information in a machine-readable format directly to another insurer.

Relatedly, the concepts of the right to access and the mechanism to provide portability are commonly confused in privacy discussions. Access is the ability of consumer to know what information is being collected about them and how it is being used. It is appropriate to provide consumers reasonable access to personal information collected by a company, and if requested, in an electronic format that can be reasonably accommodated. While data portability complements the right of access, it should be clearly distinguished from the mechanism of portability.

Opt-out

Although it is not the business practice of the vast majority of insurers, we agree that consumers should have the right to opt-out of the sale of their personal information to third parties for monetary gain.

Consumers should have control over their personal information. In fact, insurers are already leaders in offering consumers transparency into privacy practices, as well as, control over their personal information. Any law in this area must balance consumer control with a company's need to collect and share information for normal business practices. Current privacy law applicable to financial institutions does just that. Under the *Gramm-Leach-Bliley Act (GLBA)*, insurers must inform consumers about data-sharing practices and explain to consumers their rights if they do not want their information shared with certain third parties. The *NAIC Privacy of Consumer & Health Information Regulation (#672)*, which is the state insurance mechanism for GLBA implementation, requires companies to inform consumers if the company intends to disclose nonpublic personal financial information to third parties outside of specific exceptions. Moreover, companies must let the consumer know that they have the right to opt-out of that disclosure, and to provide a reasonable means by which the consumer may exercise the opt-out right. The regulation provides examples of adequate notice as well as reasonable opt-out means, including an electronic opt-out option. These provisions were drafted two decades ago when the internet was still in its nascent stage. While

updates may be warranted for new technologies, we believe that the balanced opt-out approach remains appropriate and effective to protect consumer privacy.

Again, as mentioned above, there is a need for balance in privacy rules to provide strong protections for consumers while enabling companies to obtain and use personal information in the normal course of business where the collection, use and disclosure is necessary and proportionate. GLBA, and subsequently NAIC Model #672, provide a carefully curated list of exceptions to opt-out such as with the consent, or at the direction, of the consumer or to protect confidentiality or security of the information or to protect against fraud, among other reasons,. These exceptions provide a useful starting point for the kinds of personal information companies must share to provide and service consumer insurance products.

Similarly, the *Fair Credit Reporting Act ("FCRA")* provides consumer protections for the sharing of personal financial information provided to financial services companies by consumer reporting agencies. FCRA requires insurers to notify consumers if they plan to share information with affiliates or third parties and provide an opportunity for the consumer to opt-out.

Opt-in

The very nature of the business of insurance requires that carriers collect highly sensitive personal information for the purpose of evaluating risks. Moreover, consumers authorize and opt-in to the collection of this information. As required by current financial services privacy rules and insurance law, consumers receive notice of information practices as well provide explicit consent to the collection of personal information when they apply for an insurance product.

Disclosures

As required by GLBA and corresponding NAIC Model #672, insurers are bound by limits on disclosure of nonpublic personal information to third parties. With certain permitted exceptions, companies are prohibited from disclosing any personal financial information to a third party without informing the consumer by way of notice and providing the consumer with the reasonable opportunity to opt-out of the disclosure. Similarly, the *Health Insurance Portability and Accountability Act of 1996 ("HIPAA")* and corresponding provisions in NAIC Model #672 provide significant restrictions on the disclosure and use of individuals' protected health information. Furthermore, the *HITECH-HIPAA Omnibus Rule*, adopted in 2013, expanded and strengthened HIPAA's "minimum necessary standard". The minimum necessary standard restricts the sharing of protected health information to the minimum amount necessary to fulfill the request at hand.

As articulated above, the restrictions on disclosure are already robust for the insurance industry. And while modernization may be prudent, changes will be difficult to NAIC Model #672 without amendments to the governing federal laws mentioned above.

Conclusion

Policymakers have responded to the privacy debate with varying proposals to provide consumers with greater transparency and control over the use of personal information, with California being the leading example. However, while lawmakers in California passed comprehensive new requirements for the entire business community, they did not harmonize with the existing privacy requirements applicable to the financial services industry and, in particular, insurers. In addition to the new *California Consumer Privacy Act ("CCPA")*, and its latest iteration the *Consumer Privacy Rights Act ("CPRA")*, the state also has current insurance specific privacy laws such as the *NAIC Insurance Information and Privacy Protection Model Act (Model #670)* and the *NAIC Privacy of Consumer Financial and Health Information Regulation (Model #672)*. As a result of the lack of alignment with

existing laws in California, the insurance industry is now burdened compliance with multiple and conflicting laws.

In addition to these sectoral requirements, insurers must also comply with laws such as the *Fair Credit Reporting Act ("FCRA")*, the Driver's License Protection Act, the Online Privacy Protection Act, and the California Shine the Light law when doing business in California alone. For multi-state insurance carriers, the picture is even more complicated.

As we have stated before, insurers are uniquely affected by the confluence of general consumer privacy laws and our existing regulatory scheme. The consequences of differing, overlapping and sometimes conflicting requirements – as we are seeing play out in California – will confuse consumers and may detrimentally impact the insurance industry, particularly considering the types of data insurers collect, and long history of responsible data collection and stewardship. Subjecting the insurance industry to conflicting or overlapping requirements hurts rather than helps consistency. Our greatest request is for simplicity and harmonization of consumer data privacy requirements.

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

Sincerely,

Kate Kiernan

Arbor Strategies, LLC

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

December 17, 2020

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[1] of health carriers, representing some of the country's largest major medical insurers and health maintenance organizations, commenting on the NAIC Privacy Protections (D) Working Group ("Working Group") proposed work plan. As you know, the health insurance industry has a long history of maintaining high standards of privacy protection for the information collected by our companies. As a threshold matter, the Coalition has significant concerns about leveraging European privacy models in the United States health insurance industry. Not only is privacy highly regulated by the federal government through HIPAA and the Graham Leach Bliley Act, the health insurance industry complies with over fifty state privacy laws, all designed to protect consumer data and privacy.

As the NAIC considers updates to its privacy model, we submit that there are sufficient models developed in the United States enacted in alignment with the United States system of state-based insurance regulation. This Coalition supports Working Group efforts to develop a uniform model that can be passed in the states; however, it must not undermine our existing privacy programs, which provide significant protections to health insurance consumers who are purchasing and utilizing health insurance in the United States. It is important to recognize that health insurance data is managed and used differently than non-insurance data managed and used by technology companies and other non-insurance entities. This is a key point and one which we

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

would respectfully request the Working Group take additional time with input from industry to consider before drafting specific language based on the European model.

The Coalition is concerned about the proposed workplan to the extent it presupposes that certain issues, termed "consumer issues" are, merely because of their nomenclature, automatically deemed beneficial. In fact, we suggest that many of these issues, particularly those taken from provisions of the European Union's General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act ("CCPA") will be extremely detrimental to individuals, to the coordination of health care in the United States, and therefore, overall, to society. Neither of those two privacy laws were drafted with the unique characteristics of health insurance in mind, and in fact, as noted below in more detail, were drafted to provide protections for individuals interfacing with data driven non-insurance entities like Facebook.

The GDPR generally targets big technology companies and large data aggregators, and the CCPA applies generally to the business community as a whole. Neither specifically focuses on the health insurance industry. The United States health care system and health insurance industry operates very differently from the overall business community. The health insurance industry collects, uses, and discloses health insurance information to manage patient's health care and health outcomes, and to manage health care costs for consumers. NAIC Privacy Model 672 and the privacy regulations drafted pursuant to the Health Insurance Portability and Accountability Act ("HIPAA") were carefully crafted to recognize and balance this interchange between our need to use health information and our customers' data privacy.

The health insurance industry is subject to robust privacy regulatory schemes, both at the state and federal levels, with both HIPAA and GLBA as the federal cornerstones. Before layering any additional requirements on the health care system and health insurance industry, we must all ensure that there is a clear understanding of both the intended and unintended consequences of any changes to the existing structure guiding health insurance privacy requirements. A preliminary examination of the "consumer issues" identified by the Working Group: 1) portability; 2) disclosures; 3) notification; and 4) opt-in/opt-outs suggests, as discussed below, that some if not all of these issues are inappropriate for the United States health insurance industry in light of the needs of existing consumer protections, the United States health insurance system, and robust state-based insurance regulation.

Portability

Portability, as that term in used in the GDPR and the CCPA, means something quite different from its use in HIPAA and NAIC insurance reforms models, and is inappropriate for application to the United States health insurance industry. In the EU, portability is the ability of individuals, who are data subjects to receive the personal data they have provided to a "controller" and transmit it to another controller without hindrance from the controller that presently has the

data. While this makes sense for internet service providers, for example, it does not make sense in the group or individual health insurance markets, where open enrollment periods and other protections are needed to protect the stability of the risk pool. And while the concept might work in the technology space, where individuals are free to change internet service providers at any time, there are contractual and risk management concerns that make this concept unworkable for consumers and insurers in the context of its application to our health insurance system and industry.

The GDPR portability concept operates under the assumption that the individual consumers should be able to decide with whom they conduct business, whose services they want to use, and where their information resides. Implicit in the concept is that portability addresses the concern that individuals be prevented from moving to another service provider. This harm does not exist in the health insurance industry. Employers and individuals regularly switch insurers, and individuals have the right to authorize and direct that their information be provided to another health insurer for quotes and potentially to replace coverage within the context of open enrollment periods which preserve markets and consumer options.

Disclosures

Our Coalition members support the general concept that health insurers may only disclose or use protected information if the individual that is subject to the information has authorized the disclosure or use of the information, or if the disclosure or use is otherwise permitted by law. Both Model 672 and HIPAA privacy regulation take this approach. We do not believe this general approach to the disclosure or use of protected information should be disturbed.

Opt-out vs Opt-in

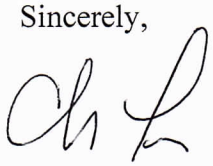
Opt-out and opt-in are frequently used when discussing privacy concerns but also seem to mean different things to different people. We will need a better understanding of what the Working Group intends by these terms before we can competently comment on this issue.

Notifications

Notifications are probably an area where everyone agrees improvements are needed, but, unfortunately, in light of the federal Gramm-Leach-Bliley Act, it is less clear what the NAIC can do about them. The Coalition supports efforts to streamline and standardize notification requirements in a way that provides consumers with the information they need at the right time. It is not clear to us that the NAIC can disturb well established existing federal requirements. We would, however, agree that the notices themselves are not likely to provide any real consumer benefit, however, the Coalition is supportive of Working Group efforts to improve these processes.

Thank you for allowing us to comment. If you have any questions, please feel free to reach out to me at either (202) 247-0316 or at cpetersen@arborstrategies.com. We look forward to working with the Working Group as it considers possible revisions to NAIC Privacy Model 672.

Sincerely,



Chris Petersen

cc: Lois Alexander

NAMIC
NATIONAL ASSOCIATION OF MUTUAL INSURANCE COMPANIES

317.875.5250 | [F] 317.879.8408
3601 Vincennes Road, Indianapolis, Indiana 46268

202.628.1558 | [F] 202.628.1601
20 F Street N.W., Suite 510 | Washington, D.C. 20001

NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

PRIVACY PROTECTIONS (D) WORKING GROUP

Request for Comments on Consumer Issues

December 22, 2020

On behalf of National Association of Mutual Insurance Companies (NAMIC)[1] members, thank you for the opportunity to review the materials under consideration by the NAIC's Privacy Protection Working Group. These comments respond to the December 4 email indicating, "one of the Working Group's next steps is to request comments from all interested parties on the Consumer Issues (Notifications, Portability, Opt-in/Opt-out, and Disclosures)." These comments are provided primarily through the lens of NAIC Model 672, *Privacy of Consumer Financial and Health Information Regulation*.[2]

Notice Content

Model provisions relating to what information should be contained in the upfront consumer notice of an insurer's privacy practices (the GLBA notice), as contained in Section 7, appear sufficient.

To the extent the Working Group elects to revise notice content provisions, NAMIC suggests:

- Optional safe harbor **sample clauses**, as was done in Appendix A of Model 672 provides useful operational guidance for insurers during implementation.
- Similarly, and as appropriate, embedding **examples** – in definitions and in substantive provisions – both affords flexibility and illustrates useful information for insurers.
- Continued allowance of a **Federal Model Privacy Form**, as was done in Appendix B of Model 672, affords additional consistency and certainty for those who elect to follow it.

These kinds of compliance aids may prove helpful in providing some additional certainty. When considering notice content, NAMIC encourages the Working Group to recognize that generally speaking consumers may be overwhelmed by an especially detailed notice – it is important to convey the high-level types of information that gives the consumer a sense of the kinds of data collected and disclosed (and to whom disclosed outside of the exceptions). The framework in the model provides these larger ways to convey the institution's privacy practices.

[1] NAMIC membership includes more than 1,400 insurance companies. The association supports regional and local mutual insurance companies on main streets across America and many of the country's largest national insurers.
[2] https://content.naic.org/sites/default/files/inline-files/MDL-672.pdf

Notice Delivery

Technology has changed over time – and with it, many customers' preferences have too. In 2000 (when Model 672 was passed initially) overall use of the internet was at 52% of U.S. adults; in 2019 (pre-pandemic) it was at 90% (the vast majority), according to the Pew Research Center.[3] Some customers may want to have the ability to review privacy policies electronically at any time for ease of use and/or as an environment-friendly alternative to paper.

Given this evolution, NAMIC recommends that the provisions in Section 11 (and perhaps elsewhere) be updated to allow notice to be delivered by providing a way to leverage allowing **web-based postings** of privacy policies (with an additional alternative available for those not having or not wishing to use the online material). Common sense approaches should be integrated into the options.

Continuing with the theme of flexibility, if a customer has multiple connections to an institution, to simplify, as appropriate, that organization should have the option to cross-reference online materials in a single effort rather than to send separate notices.

Finally, on the question of the frequency of privacy notices, recall that at first they were envisioned as annual. By way of background, in 2015 the Fixing America's Surface Transportation Act (FAST Act) amended the privacy provisions of Gramm-Leach-Bliley Act (GLBA) to eliminate the requirement of redundant annual privacy notices. In essence a financial institution would not be required to provide annual privacy notices if disclosing consistent with GLBA and if privacy policies and practices have not changed from what was described in the most recent privacy notice sent to customers. In 2016, the NAIC Privacy Disclosures Working group and the Market Regulation and Consumer Affairs (D) Committee adopted a Model Bulletin consistent with this approach.[4]

Preference Mechanism: Opt-In/Opt-Out

NAMIC strongly urges the use of opt-out (other than in the case of narrowly and specifically defined sensitive information, such as protected health information, and for certain out-of-context uses, namely marketing). In this digital age of consumer convenience, clear notices and opt-out choices should be provided, as they already are in insurance privacy notices. As drafting continues, NAMIC urges exemptions to resemble today's workable privacy structure that is effective for the regulated insurance industry and for customers of insurance products and services.

Taking a step back, the objective of providing a mechanism to protect consumers who wish to restrict information-related activity can be met under both an opt-in and an opt-out.

- No greater privacy protection is afforded under either approach to an individual wanting more restrictive data handing.

[3] https://www.pewresearch.org/internet/fact-sheet/internet-broadband/

[4] https://content.naic.org/sites/default/files/inline-files/legal_bulletin_gramm_leach_bliley_act_annual_privacy_notices.pdf

- Under both approaches the individual consumer controls the decision.

The difference is the default automatic standard and the consequences of a broad opt-in (which may have a facial appeal initially, given its apparent simplicity). However, it seems the opt-in approach may offer fewer choices to consumers because it assumes that consumers value restrictions over the benefits of product and service variety, innovation, and/or ease of use. Not only may an opt-in be more costly to administer because it would require companies to obtain consent, but customers may perceive it as more intrusive due to increasing contacts with the customer in an effort to secure consent. This may be especially true in increasingly online and mobile interactions, where opt-in requirements can result in numerous pop-up boxes that interrupt consumers' experience and service.

Imbedded in the existing comprehensive privacy framework for financial services and insurance is a general approach of opt-in for health information and of opt-out for financial information. The scope of what a consumer may choose must clearly carve out the practical business function exemptions such as: eligibility or underwriting, fraud prevention, and account-servicing or processing type tasks. Again, Title V of the GLBA[5] provides the landmark privacy framework for financial services (including insurance). It sets forth notice requirements and standards for the disclosure of nonpublic personal financial information – it specifically requires giving customers the opportunity to **opt-out** of certain disclosures.

Disclosure/Redisclosure

Model 672 focuses on insurer disclosure of nonpublic personal financial and health information. The financial provisions are based on the provisions of the Gramm-Leach-Bliley Act and it outlines when insurers may disclose and to whom. If the Working Group is considering changes, NAMIC urges that this group value the important operational needs of financial institutions.

Given the importance of data in the insurance transaction, historically, policymakers have recognized the important role information plays in insurance and they have allowed for various exemptions for operational and other reasons. There are vital business purposes for insurers to collect, use, and disclose information. The existing model regulation appears instructive on types of operational functions to preserve and facilitate. It includes functions being performed on behalf of the insurer. In addition, many of these exemptions enable insurance companies to meet consumers' expectations of convenience and ease consistent with insurance companies' contractual obligations to their individual customers.

As insurance regulators, you are aware that there are other data-related laws with which insurers are required to comply. For example, an insurer may have federal and state compliance obligations to use data in a number of ways, including reporting and/or checking against databases for things like: fraud, child support liens, Office of Foreign Assets Control (OFAC) watch list, Medicare/Medicaid reporting/liens, fire-loss reporting to state fire marshals, and theft/salvage claims reporting. These laws support important existing public policy mandates and priorities. Also, the insurance industry is subject to record retention

[5] See 15 U.S.C. Sec. 6801 et. seq.

requirements. Kindly keep these requirements in mind as the Working Group considers disclosure-related issues.

To the extent that the "disclosures" reference in the comment invitation referred to a kind of communication that is outside of Model 672, but part of a particular state's law and triggered by some additional requirement, NAMIC would like to have additional information before commenting.

Portability

Perhaps due to the context stemming from the Health Insurance Portability and Accountability Act (HIPAA), the term "portability" typically brings to mind the idea of an employee bringing health benefits with them when they change/leave a job. It may also bring to mind the concept of data being in a specific format to be transferred as one changes medical providers. The idea of "portability" is not the same as that of "access." To the extent that the "portability" reference in the comment invitation referred to a kind of issue that is outside of Model 672, NAMIC would like to have additional information and/or see language before commenting. (It may raise questions about method of designation/direction, recipient entities, security concerns, validation of entity, costs, liability, etc.)

Larger Context & Conclusion

In possible contrast to other business segments outside of the regulated industries, the existing comprehensive privacy regime has been working, with processes in place and regulators having authority to address concerns. NAMIC asks that the Working Group appreciate the complexity of the privacy regulatory landscape by integrating compliance deemers, as appropriate, to allow for sending consumers a single notice. As the NAIC Privacy Protections (D) Working Group considers possible changes to the model, NAMIC urges a deliberative discussion and cautious drafting to understand existing laws (including some referenced above that are not privacy-specific) in order to minimize conflicting laws/regulations as well as consumer and compliance confusion.

On behalf of its members, NAMIC is prepared and willing to engage on the important subject of privacy laws and regulating our industry. We look forward to working with the NAIC as the efforts of the Privacy Protection Working Group continue in 2021.

December 18, 2020

Cynthia Amann, Chair
Ron Kreiter, Chair
Privacy Protections (D) Working Group
NAIC Central Office
1100 Walnut, Suite 1500
Kansas City, MO 64106-2197

Attn: Lois Alexander, Market Regulation Manager

VIA Electronic Mail: lalexander@naic.org

RE: Privacy Protections (D) Working Group Consumer Issues

Dear Ms. Amann and Mr. Kreiter:

The American Property Casualty Insurance Association (APCIA)[1] appreciates the opportunity to provide initial feedback to the National Association of Insurance Commissioners' (NAIC) Privacy Protections (D) Working Group's (Working Group) regarding consumer issues. The comments below do not provide a deep substantive analysis, but, rather, identify some high-level observations.

Exclusivity and Interoperability

New and proposed all-industry privacy laws are well intentioned, but add an additional layer of requirements that conflict with the insurance privacy regime and do not account for unique and necessary business transactions. Therefore, the insurance industry is at risk of not only multi-state inconsistency, but also inconsistency within an individual state. These inconsistencies can result in consumer dissatisfaction and unnecessary increased corporate compliance costs.

As such, we continue to urge that the goals of this Working Group should be two-fold, promote exclusive insurance industry requirements, as well as ones that are workable and can be interoperable among multiple privacy regimes. Insurers should be able to implement workable controls across their systems and data that meet individual state requirements as well as, that promote consistency for diverse and global companies. The insurance industry has been striking this balance for decades, and the NAIC is well positioned to understand and promote this balance. For instance, opt-out sharing has worked well for the industry and consumers and the NAIC should resist the temptation to up-end this process because of high profile events from industries that are not subject to privacy laws and protections.

[1] Representing nearly 60 percent of the U.S. property casualty insurance market, the American Property Casualty Insurance Association (APCIA) promotes and protects the viability of private competition for the benefit of consumers and insurers. APCIA represents the broadest cross-section of home, auto, and business insurers of any national trade association. APCIA members represent all sizes, structures, and regions, protecting families, communities, and businesses in the U.S. and across the globe.

Consumers benefit from exclusivity and interoperability in a way that reduces consumer confusion and allows companies to focus on consumer protections as opposed to diverting resources to meet complex compliance requirements that do not enhance consumer protection.

Notice/Disclosures

Since the adoption of the Gramm Leach Bliley Act federal regulators and insurance commissioners have modernized privacy laws based on experience and consumer expectations. For example, regulators and industry have simplified the privacy notices from both content/format and frequency of distribution perspectives. The NAIC should not upend this by following comprehensive state laws in multiple notices, as well as notices that overwhelm with information.

It is important in any privacy analysis to remember more information is not always the ideal solution. Dense, complex, and prescriptive requirements can only enhance consumer confusion and prohibit businesses from having the flexibility to make meaningful changes for consumers. Too much information can also create notice fatigue rather than promote meaningful consumer choice and transparency. Where we can remove requirements that are addressed elsewhere or can be collapsed into a single requirement, APCIA is fully supportive and encourages the Working Group to consider opportunities to remove multiple layers of disclosures. Allowing for flexibility to craft consumer notices focused on categories of information collected, categories of recipients, and available rights to limit use for marketing will ultimately benefit the consumers.

On the most recent Working Group call, the idea of exploring recordings of privacy notices was identified. APCIA respectfully recommends careful and balanced consideration and exploration of what may already be available. In practice a recording requirement may prove to be unduly burdensome with very little benefit because tools may already be available to help read information posted on a website.

Opt-in/Opt-out and Portability

Consistent with notice and disclosure considerations, a risk-based approach that appropriately balances risk and operational challenges with consumer protection is critical. In practice portability requirements may sound attractive but as you begin to explore the outline for such a requirement the significant operational challenges and minimal consumer benefits may come to light. For example, is it in the consumer's best interest to start sending sensitive information through networks that could increase the potential for loss and misuse? Additionally, the proprietary nature of information must be considered.

Thank you for the opportunity to comment. As stated earlier, these are all very high-level and preliminary comments, but APCIA looks forward to constructively collaborating in more detail as the work of this Working Group advances.

Respectfully submitted,

Angela Gleason