Date: 7/12/21

Virtual Meeting

PRIVACY PROTECTIONS (D) WORKING GROUP
Monday, July 12, 2021
2:00 – 3:00 p.m. ET / 1:00 – 2:00 p.m. CT / 12:00 – 1:00 p.m. MT / 11:00 a.m. – 12:00 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 Teresa Green Oklahoma
Erica Weyhenmeyer Illinois Raven Collins/Brian Fordham Oregon
LeAnn Crow Kansas Gary Jones Pennsylvania
T.J. Patton Minnesota Don Beatty/Katie Johnson Virginia
Molly Plummer/Tyler Spady Montana

NAIC Support Staff: Lois E. Alexander

AGENDA

1. Consider Adoption of its June 14 Minutes—Cynthia Amann (MO)  Attachment 1

2. Discuss Comments Received on the Initial Privacy Policy Statement—Cynthia Amann (MO)
   • American Council of Life Insurers (ACLI)  Attachment 2

3. Hear a Presentation on Consumer Privacy—Cynthia Amann (MO)
   • Karrol Kitt—University of Texas at Austin
   • Brenda J. Cude—University of Georgia

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

5. Adjournment—Cynthia Amann (MO)
Privacy Protections (D) Working Group
Virtual Meeting
June 14, 2021

The Privacy Protections (D) Working Group of the Market Regulation and Consumer Affairs (D) Committee met June 14, 2021. The following Working Group members participated: Cynthia Amann, Chair (MO); Ron Kreiter, Vice Chair (KY); Erica Weyhenmeyer (IL); LeAnn Crow (KS); T.J. Patton (MN); Chris Aufenthie (ND); Martin Swanson (NE); Teresa Green (OK); Gary Jones (PA); and Don Beatty and Katie Johnson (VA). Also participating was: Hermoliva Abejar (NV).

1. **Adopted its May 10 Minutes**

The Working Group met May 10 and took the following action: 1) adopted its March 29 minutes; 2) discussed the draft of the initial privacy policy statement; and 3) requested comments in the form of parameters and examples on the initial privacy policy statement by June 7 for discussion during the next Working Group meeting scheduled for June 14.

Mr. Beatty made a motion, seconded by Mr. Swanson, to adopt the Working Group’s May 10 minutes (Attachment XX). The motion passed unanimously.

2. **Discussed Comments Received on the Initial Privacy Policy Statement**

Ms. Amann said the Working Group would continue to discuss the privacy policy statement on the minimum consumer data privacy protections that are appropriate for the business of insurance. She said the Working Group would focus on consumer data privacy protections other than those already in the NAIC Insurance Information and Privacy Protection Model Act (#670), the Privacy of Consumer Financial and Health Information Regulation (#672), and the Insurance Data Security Model Law (#668). She also said sections in these NAIC models concerning federal acts like the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) will be considered, if necessary, after the six consumer categories identified by the gap analysis and NAIC leadership have been addressed.

Ms. Amann said the six consumer categories identifying corresponding consumer rights that attach to notice requirements and how insurers may be subject to these requirements are:

1. The right to opt out of data sharing.
2. The right to opt into data sharing.
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.

Ms. Amann said the titles of these categories are listed as rights, as that is the way these categories were received from NAIC members; however, these titles are not to be interpreted as guarantees but as points of discussion. She also said the Working Group will not change the titles of the six consumer protection categories; rather, the Working Group would provide recommendations and examples for additional clarification to these categories. For example, she said the right to delete data would not include the deletion of factual data, such as that contained in court documents. She said the Working Group would discuss comments received since the May 10 call, which is when the Working Group requested comments from Working Group members, interested state insurance regulators, and interested parties in the form of parameters and examples on the initial privacy policy statement.

Ms. Amann said comments in the form of parameters and examples on the initial privacy policy statement received by June 7 would be discussed following some brief comments by the attendees who submitted them. She said the templates that she made will be coming out soon with functional definitions that would be used not to highlight potential areas of concern, but to point to areas where the Working Group could make recommendations to fix, reinterpret, reword, explain, or clarify.

Bob Ridgeway (America’s Health Insurance Plans—AHIP) said to summarize the comments submitted, he suggested that the Working Group retain the HIPAA safe harbor contained in Model #672 because it is pervasive in that it has permeated the entire health insurance world since 2002. He said companies have worked diligently on complying, and it affects more than
just insurance. He said it also affects doctors, providers, companies, third-party administrators (TPAs), as well as those who do business with them. He said other business associates follow them regarding how to submit and process electronic claims. He said HIPAA and the GLBA exempts or carves out insurance. He also said California has this as well, with the California Consumer Privacy Act (CCPA) covering other companies. He said HIPAA already addresses all six rights in that for opt-out or opt-in, companies are prohibited from sharing data except for treatment or payment, health care operations, or special needs. He said the opt-in had to be signed indicating what data would be shared and how. He said HIPAA is already extensive as to how to correct data. Much like the General Data Protection Regulation (GDPR), he said the right to delete is not in HIPAA because a patient’s medical history is very important when considering the care a patient will need in the future. He said access to one’s data is not a concern, as patients can get a copy of their own medical records and take them elsewhere whenever they like. He said portability means the right to accounting for old data and where health information can be sent, such as to an attorney, requires a HIPAA release. He said a recent U.S. Department of Health and Human Services (HHS) rule about the disclosure of health information will serve to restrict the use of data under 45 CFR 164.522.

Ms. Amann said it was helpful to have HIPAA citations that address health care insurance, but the Working Group would also want to address concerns state insurance regulators are hearing from consumers regarding the six categories identified, and she recommended that the Market Regulation and Consumer Affairs (D) Committee address these concerns. When Ms. Abejar asked how record retention was affected by HIPAA, Mr. Ridgeway said typical record retention was 3–5 years, but claim processing was required to be kept for a very long time. Chris Petersen (Arbor Strategies LLC) added that the coordination of benefits and proving continuity of coverage also required records to be kept indefinitely in some instances. Ms. Amann said state insurance regulators need data to be retained as well for market conduct exams, so the Working Group would need to include explanations for consumers as to why some of their data could not be deleted, removed, or created as well as how its use could be limited by the consumer. Ms. Abejar asked about cyber insurance and was given the same answer. She asked if health insurers notify consumers that the requested change has been made. Mr. Ridgeway and Mr. Petersen said the company would have to show the consumer where the change they requested had been made in the consumer’s records. Mr. Swanson asked that the cybersecurity question be revisited. He said the state’s Attorney General’s office may have to be notified, and include explanations for consumers as to why some of their data could not be deleted, removed, or created as well as how its use could be limited by the consumer. Ms. Abejar asked about cyber insurance and was given the same answer. She asked if health insurers notify consumers that the requested change has been made. Mr. Ridgeway and Mr. Petersen said the company would have to show the consumer where the change they requested had been made in the consumer’s records. Mr. Swanson asked that the cybersecurity question be revisited. He said the state’s Attorney General’s office may have to be notified, and other state laws may kick in for the consumers’ protection. As an example, he said he recently got a letter about a breach from a company that he had not dealt with in many years, so the system worked as it was intended. Mr. Ridgeway asked how consumers know companies are doing this as required by state bulletins. He suggested that such bulletins be cross referenced with the Information Technology (IT) Examination (E) Working Group, including the changes made to the Financial Condition Examiners Handbook to ensure that companies do it. Ms. Amann said consumer rights come with limitations.

Randi Chapman (Blue Cross Blue Shield Association—BCBSA) said HIPAA clearly exempts health insurance, which can be confusing; and she recommended a clarification that if health insurance companies are not exempt by HIPAA, wording should be added to NAIC models so they conform with HIPAA. She said the Working Group should not add more requirements to HIPAA.

Mr. Petersen, speaking on behalf of the Coalition of Health Insurers, said he concurs with everything Mr. Ridgeway and Ms. Chapman said. He said HIPAA was specific to the insurance industry and its uniqueness to the health insurance industry. He said HIPAA was concerned about doing harm to consumers by adding to the safe harbor already in the GLBA. He said it is necessary to recognize HIPAA as a leader and allow deletion only to correct inaccurate data, not to delete all data, as medical history is needed (especially in the emergency room) and required by record retention laws. He said portability had been addressed in California and the European Union (EU) because it is needed to move one’s data from one internet to another one so it is required there, but it is not required generally in the U.S. He said one can share a copy with state insurance regulators and law enforcement, but one cannot move the data permanently. Ms. Amann said consumer disclosure notices are not just about what information but how it is distributed or shared. She said maybe notices should only be required when a change is made. She said the Insurance Holding Company System Regulatory Act (#440) and the IT Examination (E) Working Group addressed the issue of third-party vendors by referring to them as Essential Services Providers. She said Insurtech is where she expects problems and where she has concerns because of third-party vendors or business associates, which have HIPAA responsibilities as well and are required by HIPAA to comply via their contractual relationships. She said there are anecdotal problems where the law needs more umph. Mr. Petersen said that is not realistic because people give away their information at the pharmacy and at Safeway all the time just for discounts. Ms. Amann said state insurance regulators can warn consumers, but they cannot stop consumers from making their own decisions about such trade-offs of data for discounts. She said this conversation affects all other lines of business trades, not just health insurance.

Mr. Swanson asked if most states had adopted HIPAA. Mr. Ridgeway said most states had a HIPAA carve-out or something like that already. Mr. Petersen said states had adopted Model #670, which amends access to HIPAA; Model #672, which
provides a safe harbor for health information; or some combination of the two models. Mr. Swanson asked if the Market Regulation Handbook had been examined for HIPAA compliance already. Mr. Petersen said after the GLBA was added, it asserted market conduct over privacy and examined 100 companies. Ms. Amann said underwriting and claims are useful because if states see something during the examination, they can do a privacy review at the same time. She said new situations require an understanding of how current requirements can be applied; i.e., how it can be better for consumers. Mr. Swanson said homeowners insurance is different than health insurance. He said if states do not enforce HIPAA, then the federal government will. Ms. Amann said she does not want to give the American Council of Life Insurers (ACLI) a heart attack, but she wants to put them on notice that the Working Group is moving forward with its current framework, and it will include suggested definitions and requirements or revisions where it is deemed necessary. She said the Working Group would love to have input from other trades and companies representing other lines of business, but it will move forward without it if necessary. She said NAIC staff would distribute the privacy policy statement (not a model and not a white paper) for comment. Mr. Beatty said he saw Sonja Larkin-Thorne (Consumer Advocate–Retired) on the participants lists, and he said any observations she might have for the Working Group would be useful. He said the Working Group had not heard from the Life and Annuity or Property/Casualty (P/C) folks, and he encouraged them to provide input in the form of comments, examples, etc. to avoid unintended consequences with what the Working Group comes up with on their own. Ms. Larkin-Thorne said she had been following this work personally and for the state of Connecticut. Ms. Amann said it would be great to have more input from consumer representatives and on other lines of business. She also asked Lois E. Alexander (NAIC) to reach out to them. Shelby Schoensee (ACLI) said she was just assigned by the ACLI to work with this Working Group recently. She also said she planned to submit comments soon. Ms. Amann said the Working Group would be moving quickly, as it truly wants to help consumers understand their privacy issues sooner rather than later.

Ms. Amann said the next Working Group call is scheduled for July 12.

Having no further business, the Privacy Protections (D) Working Group adjourned.
July 9, 2021

Cynthia Amann, Chair  
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

Re: Comments on NAIC Privacy Protections Working Group Initial Draft Privacy Policy Statement

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

Thank you for soliciting stakeholder feedback on your initial draft privacy policy statement exposure. The American Council of Life Insurers respectfully submits the following comments on your request for input.

As mentioned in our previous comment letters, the insurance industry has long been a consumer privacy leader in adhering to clear obligations in the appropriate collection, use, and sharing of personal information. Keeping our policyholders’ personal information private and protected is at the core of what we do. Our industry has appropriately managed consumers’ confidential medical and financial information for decades and, in some instances, over a century. As such, insurers have been subject to comprehensive federal and state privacy laws and regulations, which 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 consumers. ACLI believes consumers and companies need consistent privacy rules providing uniform protections across the country and supports establishment of a single, preemptive policy regarding the confidentiality and security of personal information.

Life insurers believe it is important for consumers to have certain rights with respect to personal information that companies maintain about them. At the same time, companies need the ability to maintain and process such personal information to provide consumers with the products and services they request, as well as to ensure the accuracy and integrity of information they use and comply with applicable laws and regulations (such as those pertaining to records retention). While modernizing existing privacy laws is arguably necessary, we should avoid creating a system which would result in additional complexity. Such complexity may result in differing consumer rights, varying levels of protections, fragmented implementation, and legal uncertainty.
We offer the following thoughts to the Privacy Protections Working Group on topics including opt-out; opt-in; correction, amendment, and deletion; portability, and right to restrict use of data.

**Opt-Out**
Life insurers believe that consumers should have control over their personal information. Current privacy law applicable to financial institutions balances that consumer control with a company’s need to collect and share information for normal business practices. 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 (Model #672)*, which is the state insurance mechanism for implementing the GLBA, 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. Additionally, the *Fair Credit Reporting Act (“FCRA”)* provides consumer protections for the sharing or use of personal information provided to financial services companies by consumer reporting agencies. FCRA requires insurers to notify consumers if they plan to share consumer report-type information with affiliates and provide an opportunity for the consumer to opt-out of affiliate sharing for marketing purposes.

Privacy rules must balance the need to provide strong protections for consumers with facilitating companies obtaining and using personal information in the normal course of business where the collection, use and disclosure is necessary and appropriate. *Model #672* provides a thoughtful list of exceptions to opt-out, such as with the consent of the consumer, to service providers under contract, to protect confidentiality, or to protect against fraud, among other reasons. These exceptions provide a useful starting point for the purposes for which companies should be allowed to share without consumer 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 often authorize and implicitly opt-in to the collection of this information. As required by current financial services privacy rules and insurance laws, consumers receive notice of information practices as well as provide either explicit or implicit consent to the collection of personal information when they apply for an insurance product.

**Correction, Amendment and Deletion**
As currently written, existing models provide consumers with robust rights to request correction, amendment, or deletion of personal information, while still allowing insurance companies appropriate leeway to decline such requests when legally or practically necessary. A key consideration is the need to maintain the integrity of the personal information companies to use to provide their products and services. This balance of life insurance companies’ needs and individual rights also generally aligns with how the *California Consumer Privacy Act (CCPA)* and *Virginia Consumer Data Protection Act (VDPA)* have addressed these issues. For example, the CCPA states that a business is not required to comply with a consumer’s request to delete personal information if it is necessary for the business to complete the transaction for which the personal information was collected, provide a good or service requested by the consumer or reasonably anticipated within the context of a business’ ongoing relationship with the consumer, perform a contract between the business and the consumer, detect fraudulent or illegal activity,
and comply with a legal obligation, among other things. The VDPA similarly states that a consumer’s rights to request access, deletion and correction of their information shall not be construed to restrict a company’s ability to, among other things, comply with laws or regulations, provide a product or service specifically requested by a consumer, perform a contract to which the consumer is a party, and prevent, detect, protect, or respond to identity theft, fraud, and illegal activity.

**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 treatment information, 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 because most insurance products are underwritten, different insurers often have different acceptance criteria, and consumers typically are able to 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. Additionally, insurers have obligations to safeguard and prevent unauthorized disclosure of consumers’ personally identifiable information. The practice of transmitting data and making it portable may also have the unintended consequence of increasing the chance for unauthorized disclosures and identity theft, which would be a potential harm to consumers.

Insurers have experienced very low request volumes 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 data 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 consumers to ask their insurer to transfer the consumers’ personal information in a machine-readable format directly to another insurer.

**Disclosures**

As discussed above, under GLBA and corresponding NAIC Model #672, insurers are bound by limits on disclosure of nonpublic personal information to third parties. For example, companies are prohibited from disclosing any personal financial information to a third party for the third party’s own business purposes without informing the consumer by way of notice and providing the consumer with the reasonable opportunity to opt-out of the disclosure. Medical information cannot be disclosed to third-parties for their marketing purposes without an actual opt-in authorization. Similarly, the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and corresponding provisions in Model #672 provide significant restrictions on the disclosure and use of individuals’ protected health information. Existing models also contain numerous restrictions and limitations relative to the disclosure of nonpublic personal information.

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

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 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. A patchwork quilt of differing state-by-state privacy regulations is confusing, frustrating, and potentially harmful to consumers. We continue to seek simplification and harmonization of consumer data privacy requirements.

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

Sincerely,

Shelby Schoensee
Associate Counsel

Kristin Abbott
Counsel