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

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

Exposure Draft

December 7, 2021

Table of Contents

I. Introduction

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

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

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

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

II. Overview of Issue

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

V. Summary of General Data Protection Regulation (GDPR)

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

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

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

VI. Summary of Recently Adopted Consumer Privacy Protection Laws

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

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

Scope

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

Exemptions

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

Consumer Rights

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

Business Obligations

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

Enforcement

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

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

B. Colorado Privacy Act (CPA)

Scope

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

Exemptions

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

Consumer Rights

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

Business Obligations

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

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

Enforcement

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

C. Virginia Consumer Data Protection Act (CDPA)

Scope

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

Exemptions

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

Consumer Rights

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

Business Obligations

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

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

Enforcement

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

VII. Summary of Working Group Discussions of Selected Key Points

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

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

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

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

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

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

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

The Working Group operated under these distinctions.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

VIII. Conclusion and Recommendations

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

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

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

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

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

Appendix A

National Association of Insurance Commissioners
Report on Consumer Data Privacy Protections

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

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

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

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

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

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

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

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

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

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

familiar terminology.

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

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

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

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

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

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

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

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

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

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

III. Consumer Access

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

IV. Data Accuracy

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

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

V. Data Ownership and Portability

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

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

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

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

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

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

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

