FIRST WORKING GROUP EXPOSURE DRAFT OF PRIVACY POLICY STATEMENT
August 30, 2021

This privacy policy statement is the framework for the minimum consumer data privacy protections that are appropriate for the business of insurance to be applied to NAIC models #670, #672, etc. as revisions, if possible, or as a start for a new model, if necessary.

It is intended to aid in completing the first step in creating a framework: defining the parameters of these rights by offering suggested definitions, examples of consumer risks, and what may not be protected in federal laws or not covered under NAIC Model laws.

The focus of the Privacy Protections (D) Working Group is on the six consumer data privacy rights or types of consumer data privacy protections 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 Privacy Protections Working Group's task is 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 opt in of data sharing

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 is also tasked to analyze or determine how insurers are protecting these rights - as a requirement by state or federal statutes, or because of the requirements imposed by the state or federal statutes.

TEMPLATE:

CONSUMER RIGHTS AND INSURER OBLIGATIONS

▪TITLE OF CONSUMER RIGHT **{1-6 below}**

▪DEFINITION

▪EXAMPLES

▪CONSUMER RISK / IMPACT

▪CURRENT STATE AND FEDERAL LAWS / RULES THAT APPLY (GLBA, HIPAA, Model Act #670, Model Regulation #672, Insurance Data Security Model-IDSM #668, etc.)

I. Review *NAIC Insurance Information and Privacy Protection Model Act (Model #670)*

A. Adopted in 1980.

B. **Seventeen states have adopted Model Act #670: AZ, CA, CT, GA, HI, IL, KS, MA, ME, MN, MT, NV, NJ, NC, OH, OR, & VA. One state did a Bulletin: AR.**

C. Sets standards for the collection, use and disclosure of information gathered in connection with insurance transactions.

1. Requires insurers to provide notice that alerts the individual of the insurer's information practices. The insurer shall provide a notice in writing which shall state:

   a. Whether personal information may be collected from persons other than the individual or individuals proposed for coverage;
   b. The types of personal information that may be collected and the types of sources and investigative techniques that may be used to collect such information;
   c. A description of the rights established under this Act and the manner in which such rights may be exercised; and
   d. 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.

2. Gives consumers the right to request that an insurer:

   a. Give the individual access to recorded personal information;
   b. Disclose the identity, if recorded, of the third parties to whom the insurance disclosed the information;
   c. Disclose the source of the collected information, if available;
   d. Correct their information; • Amend the personal information; and
   e. Delete the collected personal information.

II. Review *NAIC Privacy of Consumer Financial and Health Information Regulation* (Model #672)

A. Adopted in 1998.

B. **Most states have adopted Model Regulation #672. <u>Ten states have adopted the current version of this Model Regulation</u>: CO, DE, KY, NH, RI, SC, TX, UT, VT, & WA. <u>Thirty-two states have adopted the previous version</u>: AL, AK, AR, CA, CT, DC, FL, HI, ID, IL, IN, IA, KS, LA, MD, MI, MO, MS, ND, NE, NM, NV, NY, OK, PA, PR, SD, TN, TX, WI, WV, & WY. <u>Seventeen states have taken additional related action</u>: AZ, CA, DE, GA, LA, ME, MI, MN, MS, MT, NC. NJ, OH, OR, PR, RI, & VA.**

C. Requires that insurers provide notice to consumers about its privacy policies and practices.

D. Describes 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.

E. Provides methods for individuals to prevent a licensee from disclosing that information – "opt out" for financial info and "opt in" for health information.

F. Enforced via the state's Unfair Trade Practices Act.

III. Review *NAIC Insurance Data Security Model Act-IDSM* (Model #668)

A. Adopted in 2017.

B. **Eleven states have adopted this Model Act #668: AL, CT, DE, IN, LA, MI, MS, NH, OH, SC, & VA. Three states have taken related action: MD, NY, & PR.**

IV. Review the General Data Protection Regulation (GDPR)

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/what-are-my-rights_en

A. Consumers have the following rights under GDPR:

1. information about the processing of personal data;

2. obtain access to the personal data;

3. ask for incorrect, inaccurate or incomplete personal data to be corrected;

4. request that personal data be erased when it's no longer needed or if processing it is unlawful;

5. object to the processing of personal data for marketing purposes or on grounds relating to a consumer's particular situation;

6. request the restriction of the processing of personal data in specific cases;

7. receive personal data in a machine-readable format and send it to another controller ('data portability');

8. request that decisions based on automated processing concerning consumer or significantly affecting consumer and based on consumer's personal data are made by natural persons, not only by computers. Consumers also have the right in this case to express their point of view and to contest the decision.

V. Review California Consumer Privacy Act (CCPA)

https://content.naic.org/sites/default/files/call_materials/NAIC%20Privacy%20Research.pdf

A. Right to Requested Disclosures - Consumers have the right to request that a business:

1. disclose the categories and specific pieces of personal information collected;

2. delete any personal information;

3. disclose categories of sources the information was collected from;

4. disclose the business purpose for collecting the information; and

5. disclose the categories of third parties with whom the information is shared, and the specific pieces of personal information that was shared

B. Notice Requirement – A business must disclose the following information in an online privacy policy:

1. a description of consumers' right to request disclosures about personal information collected;

2. a description of consumers' right to request information about any sale or disclosure of their personal information;

3. a statement of consumers protection against discrimination;

4. a list of the categories of personal information collected about consumers in the past 12 months;

5. a list of the categories of personal information the business has sold in the past 12 months; and

6. a list of categories of personal information it as disclosed about consumers for a business purpose in the preceding 12 months.

VI. Review State Data Privacy Legislation

General Data Privacy Legislation Chart:

https://content.naic.org/sites/default/files/call_materials/NAIC%20Privacy%20Research.pdf

State Privacy Law Comparison Chart (revised 8/17/21):

https://content.naic.org/sites/default/files/inline-files/State%20Privacy%20Law%20Comparison%20Chart.pdf

Abbreviated Data Privacy Legislation Chart (revised 8/17/21):

https://content.naic.org/sites/default/files/inline-files/Abbreviated%20Data%20Privacy%20Legislation%20Chart.pdf

A. State privacy legislation has included the following:

1. notice requirement;
2. requirement to disclose information collected;
3. requirement to disclose shared information;
4. requirement to disclose sources of information;
5. requirement to disclosure business purpose;
6. requirement to disclosure third party involvement;
7. a consumer right to delete information;
8. a consumer right of a portable data format;
9. a consumer right to correct information;
10. a consumer right to restrict use; and
11. a consumer opt-out or opt-in standard.

▪**GAPS IN CURRENT STATE AND FEDERAL LAWS / RULES**

- **GLBA / HIPAA Comparison:** https://content.naic.org/sites/default/files/inline-files/GLBA%20HIPAA%20%20Privacy%20Comparison%20Chart_0.pdf
- **Model 670 / CCPA Privacy Comparison:** https://content.naic.org/sites/default/files/inline-files/Model%20670%20CCPA%20Privacy%20Comparison_0.pdf

▪INSURER/LICENSEE IMPACT

▪ACTIONS NECESSARY / INSURER OBLIGATIONS TO MINIMIZE CONSUMER 'HARM'

▪RECOMMENDATIONS: [Revise existing model(s) 670, 672, 668; draft new model]

1. **the right to opt-out of data sharing**
2. **the right to opt-in of 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**

---

1. **TITLE OF CONSUMER RIGHT {1 above}: The Right to Opt-Out of Data Sharing**

▪**DEFINITION:** This is simply the ability of consumers to retain control of what data can be shared and to whom. The Working Group believes the current model law is on the right path.

Section 13 of MDL 670 requires written authorization of the individual before disclosing/sharing personal or privileged information about an individual collected or received in connection with an insurance transaction. If adopted by states, consumers have an automatic opt out of data sharing unless written authorization that meets the requirements is received by the insurer.

The problem is not whether there is an opt out, the problem is whether it is clear to the consumer that they have opted in by inadvertently signing a document with very fine print regarding authorization to disclose personal or privileged information. **MDL 672** provides for the specifics of how the authorization is collected and makes sure it becomes clearer to the consumer that certain information is collected and will be shared if given authorization.

a. Definition –

i. Opt-out gives consumers the ability to direct a company not to sell/share their personal information to a third party. This "right" does not stop a company from distributing the data within the organization that collected it, even to different business units.

ii. This 'right' also does not stop all transfers to third parties as companies can continue to provide personal information to their service providers pursuant to a written contract that meets the law's requirements. Further, companies can continue to provide data that does not meet the definition of personal information.

b. Examples –

i. When a consumer signs up to log into an insurance company's website they have to uncheck a box in order not to receive features. This may include unchecking a box as well for a company not to track your website use via cookies.

ii. The insured is given notice that their information may be sold to third parties that are not related to insurance. The consumer must notify the company affirmatively that they do not want their information sold to a third party.

iii. This may also be known as consent withdrawal.

The right of the data subject to direct a business not to sell (or exchange for a commercial purpose) personal information about the consumer; implicit in the right to opt-out is that a business may share personal information, unless directed by the consumer not to do so. Most data privacy regimes require the business to notify the consumer of the consumer's right to opt-out.

The right to opt-out should not be construed to give consumers the ability to opt-out of information-sharing which is necessary to effectuate the transaction for which the information was given, or

which is necessary for legal compliance. Third parties which receive personal information from an insurer should be required by law or contract (depending on the jurisdiction of the agency enforcing the laws) to protect the confidentiality of that information, including the adoption of security measures, and observance of an election to opt-out which has been communicated to the insurer. Accordingly, insurers sharing personal information with third parties, as needed for the insurance transaction, should inform the recipient of the consumer's election to opt-out.

▪**EXAMPLES:** NAIC Model 670 §13(K); California Consumer Privacy Act (CIV 1798.120); Prop. 24 (CIV 1798.120); Insurance Code §791.13(k)

▪**CONSUMER RISK / IMPACT:** People have an inherent privacy interest in controlling the distribution of data about them. In an insurance context, consumers provide a great deal of personal information to insurers and servicers, which is often necessary for good underwriting and risk management on the part of the insurer. Personal information which may be collected in connection with an insurance transaction includes: a person's name; date of birth; driver's license number; health history and medical records; education history; employment history; military service records; banking information; address and property information, including the type and value of homes or insured structures; make, model, year, mileage, and service history of vehicles insured; travel history; hobby or activity preferences; claims or litigation history, etc.

However, consumers have an inherent privacy interest in their information, notwithstanding its use in connection with the insurance transaction. When consumers hand over personal information to an insurance entity, they expect the information to be used in connection with the policy and aren't contemplating that insurers or other insurance entities will sell or share that information for use in unrelated commercial transactions.

Aside from consumers' inherent interest in the privacy of their information, consumers have a compelling security interest in minimizing the distribution of their personal information. Data breaches are a fact of our connected world. The right to opt-out allows consumers to reduce the distribution of their personal information, meaning that there are fewer opportunities for that information to be accessed or stolen by unauthorized parties. When a consumer provides personal information to an insurer, they have some idea of the company they are dealing with and whether they trust the security practices of that company; however, consumers have no idea about which companies are purchasing their information and what the security practices of those companies are.

The Right to Opt-Out should not be implemented in a way that causes tension with the servicing of the insurance policy. Insurers need to be able to share personal information with servicing entities, including third-party underwriters, claims handlers, anti-fraud personnel, etc. For that reason, the Right to Opt-Out should only encompass uses of personal information which are not related to servicing of the insurance policy. However, parties receiving personal information from a consumer who has opted-out should be notified by the transferring entity of the consumer's

election to opt-out, and be prohibited, either by law or contract, from further distribution of that information.

In order to ensure that consumers are aware of their rights, implementation of the Right to Opt-Out should require notice to the consumer of that right, upon initial collection of the person's personal information, and at intervals thereafter.

Implementation of the Right to Opt-Out should ensure that insurers cannot discriminate or retaliate against insureds who exercise their right. (In fact, anti-discrimination rules should apply to all privacy rights afforded to the consumer). A consumer's decision to opt-out of personal information sharing bears no relationship to the risk underwritten by the insurer; consumers should not pay higher premiums, incur additional charges, face denial of coverage, or otherwise be subject to less favorable treatment than consumers who allow sharing of personal information.

The Right to Opt-Out implies the right of the consumer to opt back into personal information sharing after having elected to opt-out. Implementations of the Right to Opt-Out often specify that a consumer's election to opt-out is of unlimited duration and that, upon receiving a consumer's election to opt-out, a business may not send opt-in requests to the consumer for a certain period of time (and specified intervals thereafter). This prevents consumers from being flooded with opt-in requests.

The Right to Opt-Out is an essential aspect of privacy. Consumers should have the legal ability to control distribution of their information, both as an aspect of their interest in their personal information, and as a means of ensuring the security of that information.

▪**CURRENT STATE AND FEDERAL LAWS / RULES THAT APPLY (GLBA, HIPAA, 670, 672, IDSM-Insurance Data Security Model #668, etc.):** The following federal statutes are in effect:

1.) **HIPPA: The Health Insurance Portability and Accountability Act of 1996** is applicable to:

a.) Health care providers

b.) Health plans

c.) Healthcare clearing houses

d.) Business associates – a person or organization other than a member of a covered entity's workforce using or disclosing individually identifiable health information to perform or provide functions, activities, or services for a covered entity. These functions, activities, or services include claims processing, data analysis, utilization review, and billing.

** Individually identifiable health information" is information, including demographic data, that relates to:*

- ✓ *the individual's past, present or future physical or mental health or condition,*
- ✓ *the provision of health care to the individual,*
- ✓ *or the past, present, or future payment for the provision of health care to the individual,*
- ✓ *and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).*

2.) **GLBA-Gramm Leach Bliley Act** is applicable to financial institutions (which includes all insurers). Financial institutions are required to give their customers (and consumers) a clear and conspicuous" written notice describing their privacy policies and practices and for the consumers to be provided with reasonable means to opt out before their non-public information is disclosed to non-affiliated parties.

Non-public financial information includes:

- ✓ any information an individual provides to a financial institution to get a financial product or service (for example, name, address, income, Social Security number, or other information on an application).
- ✓ any information provided to a financial institution about an individual from a transaction involving a company's financial product(s) or service(s) (for example, the fact that an individual is consumer or customer, account numbers, payment history, loan or deposit balances, and credit or debit card purchases); or
- ✓ any information provided to a financial institution about an individual in connection with providing a financial product or service (for example, information from court records or from a consumer report).

Analysis: The following should be noted:

1.) While **HIPAA** protects the disclosure of identifiable health information by health care providers, health plans, health care clearing houses, and business associates, not all insurance companies are health plans as defined by HIPAA and not all types of insurers are person or organizations using or disclosing individually identifiable health information to perform or provide functions, activities, or services for a covered entity. If this is a framework for the insurance industry, the Working Group needs to investigate what would apply to those not covered by HIPAA. (i.e. access, amendment of information, disclosure accounting, restriction requests…etc.) 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.

While our comments represent the health insurers' perspective, it is also important to note that our responses also reflect the views and needs of our members' enrollees. Further, since health insurers' operations in matters including, but not limited to privacy, data security, claims payments, and quality measurement are extensively regulated by the Health Insurance Portability and Accountability Act (HIPAA), the Privacy and Security Rules (45 C.F.R. Parts 160, 164), the Health Information Technology for Economic and Clinical Health ("HITECH") Act (Pub. L. No. 111-5) and the 2020 Interoperability and Patient Access Final Rule (85 FR 25510) ("Interoperability Rule"), most of our comments will refer to existing requirements under those regulations. A HIPAA Covered Entity is prohibited from using or disclosing an individual's protected health information unless the information is to be used or disclosed for an allowed purpose such as treatment, payment, or health care operations or otherwise permitted or required by policy-based exemptions in the Privacy Rule (45 CFR 164.502(a), and 45 CFR 164.508). For these purposes, neither HIPAA nor HITECH mandates either an opt-in or an opt-out approach. An individual's written authorization is required for additional uses or disclosures.

HIPAA contains robust existing consumer data privacy protections and continues to evolve to meet the needs of consumers and the technological advances in the health care sector.1 As covered entities under HIPAA, health insurers are subject to these protections and have implemented physical and administrative safeguards to protect individuals' health information. Deference to HIPAA's regulatory and enforcement regime around consumer data privacy protections is appropriate given the extent to which the health insurance industry must: 1) protect health information when using and disclosing protected health information; 2) only use such information for treatment, payment, and health care operations (unless individual authorization is obtained); and 3) adhere to consumer rights standards that have been in place for decades. Therefore, the Draft Policy Statement should include language around scope of applicability to carve out health insurers from any potential consumer data privacy standards that may be applied to NAIC model #672 as revisions (or as a start of a new model). Adding an additional layer of consumer data privacy requirements through an NAIC model update (or new model) would be duplicative, confusing to both consumers and health insurers, and add administrative burden and costs without adding meaningful protections for consumers.

To the extent that the Draft Policy Statement and any eventual model changes extend consumer data privacy requirements to health insurers, such model requirements should not go beyond existing requirements under HIPAA. Alignment with HIPAA will ensure that the same robust privacy protections apply to the same type and use of health information, no matter the jurisdiction. Doing so will mitigate duplication and conflict between federal and state requirements to prevent confusion, potentially differing interpretations, and burden among health insurance industry stakeholders and consumers.

The following reference guide addresses how HIPAA regulates health insurer requirements regarding the consumer rights identified in the Draft Policy Statement as well as the notice requirements pertaining to informing consumers of such rights.

Existing privacy requirements to which health insurers are subject provide significant protections for consumers with respect to data sharing. The HIPAA Privacy Rule imposes stringent requirements. The general rule is that protected health information (PHI) cannot be used or disclosed by health insurers as covered entities *unless* specifically permitted by federal regulations. HIPAA permits health plans to use and disclose PHI for treatment, payment, and health care operations purposes without individual authorization. Any use or disclosure of PHI beyond these purposes must be supported by a specific authorization by the individual. This authorization (opt-in) requirement, which is addressed in more detail in the next section, effectively means that the default operating procedure for health insurers is to assume that a consumer opts out of, or restricts, data sharing for any purpose not linked to treatment, payment or health care operations or as otherwise required by law (e.g., disclosure to the Department of Health and Human Services pursuant to an investigation or enforcement action).

Furthermore, for public policy to be effective at combatting the substance use disorder (SUD) and mental health crisis facing the nation today, policymakers must allow for use and disclosure of SUD and mental health-related information for treatment, payment and health care operations including care coordination. While SUD records have historically been more restricted under federal and state law, there has been an evolution in favor of sharing this information because of reduced stigma. Federal and state policymakers and diverse stakeholders are working in this direction, and there is wide consensus that alignment of substance use disorder information protections with HIPAA is the best path forward (e.g., without requiring special authorization). Pending federal rules would allow covered entities to more freely use and disclose PHI in scenarios that involve SUD, serious mental illness, and emergency situations as well as when disclosures are in response to a "serious and reasonably foreseeable threat" in recognition that access to this information will ultimately benefit the patient and their caregivers.

Consumer Notice Requirement for Right to Opt Out: A consumer's right to opt out of (or restrict) data sharing is already required to be communicated under HIPAA. First, if a health insurer has executed a valid authorization to use and disclose PHI for a purpose beyond treatment, payment and health care operations, the valid authorization must provide the individual with a right to revoke their authorization at any time, provided that the revocation is in writing, except in two very narrow circumstances: (1) the health insurer has taken action in reliance thereon; or (2) if the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.

Second, a Notice of Privacy Practices (NPP) is required under HIPAA. This notice, which must be made available to health plan members at the time of enrollment, describes, among other things, the right an individual has to restrict the use and disclosure of their PHI for even core treatment, payment, and operations purposes, as provided by the HIPAA Privacy Rule. A health insurer, like any covered entity, is not required to agree to a requested restriction, unless specifically required to by the Privacy Rule. Indeed, health plans must exchange basic member information to providers in order to accurately process claims and keep accurate records on an ongoing basic. Having inaccurate member information would jeopardize the integrity of an audit or oversight of safeguards. A covered entity must agree to restrict a disclosure about an individual to a health plan if the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and the PHI pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full. Health plans also voluntarily honor requests to restrict disclosure of PHI in cases when doing so would respect a member's request for privacy while not hindering health plan operations and record keeping, such as in the case of a younger adult on a family's policy who requests that explanation of benefits (EOBs) is not sent to a parents' residence. In addition to providing the NPP at the time of enrollment, health plans must notify individuals covered by the plan of the availability of the NPP and how to obtain it at least once every three years.

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 Gramm 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 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.

The Coalition is concerned about the potential ramifications that these "consumer issues" might have on the health insurance industry, particularly those "consumer issues" that were lifted from provisions of the European Union's General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act ("CCPA"). The health insurance industry is already subject to a robust privacy regulatory scheme. Before layering any

additional requirements upon the health insurance industry, the Working Group must have a clear picture of the unintended and the intended consequences, to both the delivery and regulation of health care and insurance, of adding these other requirements.

The United States Department of Health and Human Services ("HHS") recently published comments that share our concerns regarding well-intentioned, but potentially ill-conceived privacy regulation. In the executive summary to its proposed modifications to the HIPAA privacy rule, the HHS specifically warns that when done improperly, privacy rules "could present barriers to coordinated care and case management-or impose other regulatory burdens without sufficiently compensating for, or offsetting, such burdens through privacy protections." HHS also warns that the unintended consequences of privacy rules that fail to consider all the nuances of our health care system could "impede the transformation of the health care system from a system that pays for procedures and services to a system of value-based health care that pays for quality care."

HHS raises these concerns, in part, because of the unique nature of health insurance, the regulation of health information and the interconnectivity of health insurance, health care providers and the health information that they share. HHS is properly concerned that otherwise well-intentioned regulation of health information could instead harm consumers by negatively impacting the coordination of care and case management. We believe that HHS' concerns regarding unintended consequences highlight and further justifies the NAIC' s earlier decision to include a HIPAA privacy safe harbor in its most current privacy model.

The NAIC included a very important and well-established protection for carriers that comply with the federal HIPAA-privacy requirements in Model 672. That model provides that “[I]rrespective of whether a licensee is subject to the federal Health Insurance Portability and Accountability Act privacy rule as promulgated by the U.S. Department of Health and Human Services [insert cite] (the "federal rule"), if a licensee complies with all requirements of the federal rule except for its effective date provision, the licensee shall not be subject to the provisions of this Article V."

The HIPAA compliance safe harbor provides carriers with the ability to administratively streamline and implement one comprehensive privacy standard across all health information for all states, while at the same time ensuring that consumer information is protected on a consistent basis under the stringent privacy standards established under HIPAA. The HIPAA privacy standards are constantly evolving to meet the current needs of the environment and aim to reflect the most current thinking on protecting consumer information, while at the same time ensuring that no damage is done to the provision and financing of health care, thus providing consumers with the highest privacy and consumer protection standards.

It is also important to note that the HIPAA compliance safe harbor is simply that-a safe harbor. It is a strong, consistent foundation that works well with state oversight. If a carrier

is not compliant with HIPAA standards, the safe harbor disappears, and the carrier is subject to appropriate state standards and oversight. It is critical that any privacy model that the NAIC develops includes a safe harbor for HIPAA privacy rule compliance. As noted above, HHS is concerned with the unintended consequences of well-intentioned privacy regulations. As regulators of the health insurance industry, the members of the Working Group should also be concerned about the possible impact that implementing some of these suggested topics would have on the health insurance industry and the consumers they serve.

Many of those topics, while described as " consumer friendly", violate existing state consumer protection laws. For example, although it appears that a "right" to have information deleted would be "consumer friendly", it likely runs counter to existing state insurance laws to maintain and protect information. These requirements to maintain information are in place to ensure that insurance regulators can, among other things, enforce state insurance consumer protection laws. It also appears that a " right " of information portability i.e., the right to move information from one entity to another, if coupled with a "right" to deletion, also violates insurance laws requiring carriers and regulators to have direct access to information for market conduct, fair trade practices review and other regulatory investigations.

Before addressing the topics above and their potential unintended consequences, we note that each of these areas is improperly expressed as an absolute " right." That is, individuals have the right to amend information or the right to delete information. Emphasis added. Existing insurance privacy laws, for good reason, do not express these actions as absolute "rights".

Rather, they are expressed as a right to request an action, e.g., individuals have the right to request their information be amended. This is true for both the HIPAA privacy rule and the NAIC's Model 672. For example, under existing rules, if individuals believe there is inaccurate information in their health insurance files, they may request that this information be amended. However, if after investigation the health insurer determines that the information is accurate, then the health insurer has the right to deny the request to amend the information. In fact, health insurers may be required by law to deny the request under state insurance laws mandating those insurers maintain accurate and complete medical information and records.

The Coalition requests a better understanding of what the "right" to "opt out of data sharing" entails before we can competently comment on this issue. There is a range of possibilities. For example, it could mirror the limitations outlined under the GLBA privacy rules, under which individuals are given the right to opt-out of certain disclosures (once again, note that this is not an absolute right, but is limited to certain types of disclosures, and only if certain conditions are met). Model 672, which was designed to implement the GLBA privacy requirements, uses the term opt-out as part of its limitation on disclosures

of nonpublic personal financial information to nonaffiliated third parties. It provides that licensees may not, directly or through any affiliate, disclose any nonpublic personal financial information about a consumer to a nonaffiliated third party unless certain requirements are met.

Alternatively, the opt-out referenced above could be referring to a right under the HIPAA privacy rule giving individuals the right to request restrictions regarding the use and disclosure of their protected health information as it relates to treatment, payment, or health care operations, and the right of individuals to request restrictions for other disclosures, such as those made to family members, none of which are absolute " rights."

Health plans provide both of the rights described above as part of complying with state and HIPAA privacy laws and health plans must be permitted to continue to craft the clear and precise opt-out rights already provided for under state and federal law. We urge the Working Group to craft an exemption for health carriers that are compliant with HIPAA and applicable state laws.

2.) Most insurers may be subject to **GLBA**. However, Privacy policies and practices are still created and controlled by financial institutions. An individual's data may not be portable and merely describing the data and information that could be disclosed is not the same as access to data. The right of data sharing is provided under GLBA with no opt-out if the sharing with affiliates. Consumers may opt-out of sharing with non-affiliated third parties. There is some restriction of the right to use certain data provided by GLBA. Virginia may be open to discussions about extending this right in certain circumstances.

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.

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*.

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.

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. 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.

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.
- 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 GLBA5 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 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.

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.

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.

3.) Some states may have adopted portions of **NAIC Model Act 670**. The rights granted by this model act are:

a. **Right of access and correction** to all personal information collected (Section 8) – However, access is not automatic. With respect to the rights to correct and delete information, Virginia law currently provides such rights if the information is incorrect. These rights are included in Model #670 that was adopted by Virginia.

b. **Right to file a statement whenever an individual disagrees with an** insurance institution's, agent's, or insurance support **organization's refusal to correct, amend or delete recorded personal information**. (Section 9)

c. **Right to either be provided with specific reason or reasons for the adverse underwriting decision** in writing or advise the consumer that upon written request, he/she may receive the specific reason or reasons in writing (Section 9 – with a caveat that if adverse underwriting decision was given orally that the explanation of reasons and summary of rights may be given orally as well)

d. **Right to be provided with a summary of rights**. (Section 9)

e. **Right to know specific items of personal and privileged information that support an adverse underwriting decision.** (Section 9 – but with a caveat that insurer shall not be required to furnish specific items of privileged information if it has reasonable suspicion that the applicant is engaged in criminal activity and specific items of medical record supplied by medical care institution or medical

professional shall be disclosed either directly to individual whom the information relates to or to a medical professional designated by the individual it relates to)

f. **Right to be provided with a copy of the statement of charges, notice, order, or other process in case where a consumer's right has been violated** (Section 15)

g. **Right to certain information to be disclosed** (Section 13)

4.) **NAIC Model Reg 672** governs treatment of non-public personal health information and non-public personal financial information about individuals by all licensees of the state insurance department. This rule targets specific information within the insurance industry that requires protection supporting HIPAA and GLBA and includes provisions that are left out by HIPAA and GLBA. 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. With respect to entities subject to GLBA and any GLBA information, NAIC Model #672 must provide at least as much protection to consumers as GLBA to avoid federal preemption. Medical information cannot be disclosed to third parties for their marketing purposes without an actual opt-in authorization. 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.

5.) **NAIC Model Reg 673** establishes standards for developing and implementing administrative, technical. and physical safeguards to protect the security, confidentiality and integrity of customer information supporting GLBA and providing specific requirements for security, confidentiality, and integrity of data.

6.) In addition to looking at these federal laws, each state will need to consider any state consumer data protection laws that its legislative body has passed. For example, with respect to changes in Virginia's privacy laws applicable to the insurance industry and their customers, Virginia will take guidance from the VCDPA when considering additional protections than provided by any applicable federal law. For example, the right of data portability is not addressed in GLBA. When considering whether to apply this right to GLBA entities and their customers, we will consider the VCDPA for guidance in how the General Assembly might view that right.

7.) Another law to consider is our **Uniform Electronic Transactions Act** that provides that consumers have the right to opt-in to electronic communications. Virginia did make one exception to this requirement (with a caveat) in Section 38.2-325 D of the Code of Virginia. That provision allows insurers to post policyholder forms on their website instead of

mailing them without gaining permission from policyholders to conduct business electronically. However, insurers must mail the forms if requested by the policyholder.

▪**GAPS IN CURRENT STATE AND FEDERAL LAWS / RULES:** Insurance Code 791.13(k) do not permit an insured to completely opt-out of information-sharing for marketing purposes.

▪**INSURER/LICENSEE IMPACT:** A Right to Opt-Out creates administrative burdens on an insurer, because it requires the insurer to provide notice to the consumer, track the election of the consumer, and to manage personal information held by the insurer accordingly. To the extent that consumers opt-out of data sharing, there may be a decrease in insurer revenues from data sale, or a decrease in the ability of insurers to participate in joint marketing/bundling of noninsurance products or services. Depending on the applicable privacy rules, a Right to Opt-Out may create liability on the part of insurers who have failed to manage personal information consistent with the election of the consumer. Insurers which share personal information should require the recipient to protect the confidentiality of that information and limit disclosure consistent with the election of the consumer.

How would the company know that the authorization is from the actual insured? What are the steps to verify that information and affirmatively identify?

▪**ACTIONS NECESSARY / INSURER OBLIGATIONS TO MINIMIZE CONSUMER 'HARM':** Insurers should provide notice to consumers making them aware of their right to opt-out. As discussed above, insurers will need to provide notice to the consumer, and develop methodologies for tracking consumer choices and managing personal information accordingly. To the extent that personal information is shared as required to effectuate the insurance transaction, notwithstanding the consumer's election to opt-out; the insurer should ensure that recipients are aware of the election to opt-out and do not further share the personal information.

▪**RECOMMENDATIONS:** Consumers should be afforded a comprehensive right to control the use of their personal information for purposes unrelated to the insurance transaction. Rules adopted regarding the Right to Opt-Out should ensure that consumers are provided notice of their rights and are able to easily exercise their rights (e.g.: a requirement that insurers provide conspicuous means on their website for consumers to exercise the Right to Opt-Out). The Right to Opt-Out should be drafted so that exercise of the rights does not interfere with the transaction for which personal information was provided or hinder legal compliance. Third-party recipients of personal information should be required to take reasonable measures to protect the confidentiality of that information and limit distribution of that information, consistent with the election of the consumer. In order to ensure that consumers are free to exercise their Right to Opt-Out, the right should be accompanied by a prohibition against discriminating against consumers who have exercised their right; the availability and cost of insurance products and services should not be affected by the consumer's election to opt-out.

Life insurers believe that consumers should have control over their personal information. Current privacy law applicable to financial institutions balances 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.

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 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.

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.

---

2. **TITLE OF CONSUMER RIGHT {2 above}: The Right to Opt-In of Data Sharing**

▪**DEFINITION:** This right is similar to the right to opt out. The ability to control information should belong to the person who owns the personal information even if the information is in someone else's database for their own business purposes.

Section 13 of MDL 670 requires written authorization, that is in effect opting in if the consumer allows the sharing of information in writing.

An insurance institution, agent or insurance support organization shall not disclose any personal or privileged information about an individual collected or received in connection with an insurance transaction unless the disclosure is:

- With the written authorization of the individual (Opt-in)

Exceptions: Personal information disclosed to a person other than an insurance institution, provided such disclosure is reasonably necessary:

- To enable the person to perform a business, professional or insurance function for the disclosing institution

- To detect or prevent criminal activity, fraud, material misrepresentation or material nondisclosure in connection with insurance transactions

- To a medical care institution or medical professional for the purpose of verifying insurance coverage or benefits

- To an insurance regulatory authority

- To a law enforcement or other governmental authority

The "Right to Opt-In," means that businesses may not share personal information, unless the data subject has manifested an intention to permit sharing of their information. Implementations of the Right to Opt-In typically require "unambiguous" consent by the consumer (e.g.: receipt of the product or service cannot be conditioned on opting-in; a business cannot infer intention from a pre-checked opt-in box, etc.). Sharing of personal information which is necessary to effectuate the insurance transaction should be allowed, notwithstanding the Right to Opt-In.

In some implementations, the Right to Opt-In is formulated as a prohibition against sharing of personal information, unless the party seeking to share the information has sought and obtained the consent of the data subject.

In practice, the Right to Opt-In involves most of the same practical considerations as the Right to Opt-Out.

Note that the Right to Opt-In may also relate to the right of a consumer who has exercised their right to opt-out to subsequently opt back in to sharing of personal information.

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.

a. Definition – Opt-in is the process used to describe when a positive action that is required by a consumer in order to receive information from a company via electronic means rather than a hard copy of the document. This cannot be re-ticked boxes, opt-out boxes or other default settings.

b. Examples – When a consumer signs up to log into an insurance company's website they have to check a box in order not to receive features. This may include unchecking a box as well for a company not to track your website use via cookies.

▪**EXAMPLES:** NAIC Model 670,§13(A); CA Civil Code §1798.24(b); GDPR

▪**CONSUMER RISK / IMPACT:** The Right to Opt-In is the inverse of the Right to Opt-Out; in practice a Right to Opt-In offers greater protection to personal information, because no sale or sharing of personal information is permitted unless a consumer has elected to permit the sharing. Whereas a Right to Opt-Out allows sharing of personal information to occur, unless the consumer elects to opt-out, the Right to Opt-In prohibits sharing of personal information unless the consumer has elected to opt-in. Arguably, the Right to Opt-In is appropriate for insurance transactions, where personal information is necessary for proper underwriting by the insurer, but commercial sharing of personal information is not a necessary aspect of the insurance business (Cf. social media companies, where sharing of personal information is a core aspect of the business model). As

implemented in the CCPA/Prop. 24, the Right to Opt-In applies to minors (CIV §1798.120(c)), whereas the Right to Opt-Out applies to adults.

▪**CURRENT STATE AND FEDERAL LAWS / RULES THAT APPLY (GLBA, HIPAA, 670, 672, IDSM-Insurance Data Security Model, etc.):** A HIPAA Covered Entity is prohibited from using or disclosing an individual's protected health information unless the information is to be used or disclosed for an allowed purpose such as treatment, payment, or health care operations or otherwise permitted or required by policy-based exemptions in the Privacy Rule (45 CFR 164.502(a), and 45 CFR 164.508). For these purposes, neither HIPAA nor HITECH mandates either an opt-in or an opt-out approach. An individual's written authorization is required for additional uses or disclosures. Under HIPAA, an individual must generally authorize (or opt in to) data sharing if a health plan intends to use or disclose data beyond treatment, payment, or operations purposes, is not required by law, and is not otherwise permitted by HIPAA without individual authorization. The purposes for which individual authorization is required is addressed in detail in the Privacy Rule. Specifically, a health insurer must obtain an individual's authorization for:

1. Marketing purposes, except for a communication in the form of a face-to-face communication or a promotional gift of nominal value

2. Sale of PHI, in which case the authorization must inform the individual that the health insurer will receive remuneration for the sale

3. Use or disclosure of psychotherapy notes (relevant exceptions are made to carry out certain treatment, payment, or health care operations or in connection with legal actions).

In other words, the default assumption is that a consumer restricts and, therefore, must opt in to uses and disclosures of PHI that is not essential to the nature of health insurance.

Consumer Notice Requirement: As mentioned above, a consumer's right to opt in to data sharing by providing an authorization is already required by HIPAA. Further, health insurers must adhere to detailed documentation requirements, such as describing the class of persons who will receive the information, the expiration date of the authorization, the individual's right to revoke the authorization after initially providing it, and the potential for redisclosure of the information by the recipient, among other elements.

Additionally, the National Purchasing Partners-NPP must address an individual's right to opt into data sharing through authorization. Specifically, the NPP must describe the types of uses and disclosures that require an authorization, state that other uses and disclosures not described in the NPP will be made only with the individual's written authorization, and state that the individual may revoke an authorization.

The Coalition requests a better understanding of what the Working Group intends by the " right" to "opt-in of data sharing" before fully commenting on this issue. Health insurers presently disclose or "share data" under authorizations provided by individuals or as required o permitted by law. Obviously requiring individuals to opt-in to disclosures that are required by law or that are necessary for are the treatment, payment or health care operations would be extremely problematic and would appear to be contrary to public policy.

▪GAPS IN CURRENT STATE AND FEDERAL LAWS / RULES

▪**INSURER/LICENSEE IMPACT:** As with a Right to Opt-Out, the Right to Opt-In creates administrative burdens on the insurer, consistent with providing notice to the consumer and tracking consumers' elections with respect to sharing of their personal information. Insurer revenue from sale of personal information, or participation in cross-promotion of non-insurance products is likely to decrease more significantly as compared to a Right to Opt-Out.

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.

How would the company know that the authorization is from the actual insured? What are the steps to verify that information and affirmatively identify?

▪**ACTIONS NECESSARY / INSURER OBLIGATIONS TO MINIMIZE CONSUMER 'HARM':** Insurers should provide notice to consumers making them aware of their right to opt-in. As discussed above, insurers will need to provide notice to the consumer, and develop methodologies for tracking consumer choices and managing personal information accordingly. To the extent that personal information is shared as required to effectuate the insurance transaction, even if the consumer has not opted-in; the insurer should ensure that recipients are aware of the consumer's election and do not further share the personal information.

▪**RECOMMENDATIONS:** Given the significant amounts of personal information required for proper insurance underwriting, a Right to Opt-In is appropriate for personal information held by insurers and insurance support organizations.

---

3. **TITLE OF CONSUMER RIGHT {3 above}: The Right to Correct Information**

▪**DEFINITION:** This right ensures that underwriting process and claims adjudication will result in a fair and reasonable decision based on accurate information.

Section 9 of MDL 670 requires written request from an individual to correct, amend, or delete the portion of recorded person information in dispute. Companies still have the right to refuse to make such correction, amendment, or deletion based on lawful limitations.

The right of a data subject, after reasonable efforts by a business to verify that person's identity, to request correction of inaccurate personal information.

Implementations of the Right to Correct will often specify that, upon receipt of a request for correction and having made the correction, the business provide notice of the correction to third parties which either provided to the business, or received from the business, the information subject to correction.

Consumers may be mistaken in their belief that information is inaccurate, or may take issue with information that, while disagreeable to the consumer, is factually correct. Therefore, the Right to Correct should not require an insurer to alter information which is proved to be correct. Implementations of the Right to Correct will often specify that, if a business refuses a consumer's request to correct personal information, the business is required to notify the consumer of that decision and the bases for that decision, and to permit the consumer to file a statement setting forth why the consumer disagrees with the business' refusal to correct the information, and what the consumer believes to be the correct information; businesses are then required to ensure that the consumer's statement is available to entities accessing the disputed information.

a. Definition –A consumer may request to correct their personal information if it is inaccurate.

b. Examples – Commonly found in credit scores or FRCA data.

i. If it is determined through the dispute resolution process set forth in the federal Fair Credit Reporting Act [Pub. L. 90-321; 15 U.S.C. 1681i(a)(5)] that the credit information of a current insured was incorrect or incomplete and if the insurer receives notice of such determination from either the consumer reporting agency or from the insured, the insurer shall re-underwrite and re-rate the consumer within thirty days of receiving the notice. NOTE: This example does not encompass all data.

- A consumer's auto rate is higher because of a bad insurance score based on incorrect FRCA data. The consumer can correct the incorrect FRCA data, and the policy must be re-rated.

▪**EXAMPLES:** NAIC Model 670,§9; Civil Code §1798.106 (Prop. 24); Insurance Code §791.09

▪**CONSUMER RISK / IMPACT:** Information about a consumer may become inaccurate for any of a number of reasons, including a change in the consumer's circumstances, failure by a data source to update the consumer's data, or transcription or data entry errors. Data which do not apply to a consumer may become incorrectly associated with the consumer in a number of ways, including misattribution of information belonging to a consumer with a similar name or who lived

at a similar address, or transcription or data entry errors. This issue may become more prevalent as the number of data brokers and sources increases, and automated (e.g.: algorithmic) processes are increasingly used to collect and associate data with an individual in the absence of human oversight.

In practice, data sources may be of varying quality and accuracy, depending on the practices of the data aggregator. Consumers do not have control over information gathered about the consumer; privacy rights schemes do not typically allow the consumer to limit data sources which may be used by a company with which the consumer does business. However, consumers may suffer real and significant impacts as a result of inaccurate information being associated with the consumer. In an insurance context, these impacts may include: cancellation or denial of coverage, premium increases, etc.

▪**CURRENT STATE AND FEDERAL LAWS / RULES THAT APPLY (GLBA, HIPAA, 670, 672, IDSA-Insurance Data Security Model, etc.):** 45 CFR §164.526 (HIPPA). HIPAA already provides an individual with the right to amend incorrect or inaccurate information. 45 CFR 164.526. Under HIPAA, an individual already has the right to correct (amend) PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set. As a covered entity, the health insurer must act on the individual's request for an amendment no later than 60 days after receipt of such a request. Any denial to correct by the health insurer must have a basis authorized by the regulation and be communicated to the individual. If the individual disagrees with the denial, the individual may file a statement and/or a complaint to the health insurer or the Department of Health and Human Services. Otherwise, the information must be corrected in the manner provided in the regulation, such as through informing recipients of the corrected information including business associates.

Consumer Notice Requirement: The HIPAA-required Notice of Privacy Practices described in detail above must address an individual's right to correct information held by the health insurer.

Health plans are already subject to a similar requirement under the HIPAA privacy rule. This provision provides that covered health plans must permit individuals to request that the health plan amend protected health information maintained in a designated record set. The rule sets out additional requirements as to when and whether the health plan must amend the information and other procedures. For example, while an individual can request that certain information be removed from a medical record, if that information is correct, then in order that appropriate care be given, it is critical that the information not be deleted or amended. Again, we suggest that health plans that are HIPAA compliant are already providing the appropriate " right" regarding correction or amendment and should be exempt from any additional regulation which may ultimately hinder the provision of health care and health care financing.

▪GAPS IN CURRENT STATE AND FEDERAL LAWS / RULES

▪**INSURER/LICENSEE IMPACT:** The Right of Correction benefits insurers by ensuring that insurers have access to the most up-to-date information, meaning more accurate underwriting of risk. The Right of Correction imposes administrative burdens on the insurer, including: providing processes by which the consumer may request correction, verification of the identity of the requestor, and verification of the truth of the fact or facts in dispute.

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.

How would the company know that the authorization is from the actual insured? What are the steps to verify that information and affirmatively identify? And what's the scope for correcting, amending, or deleting information – is the deletion from the original source or also from databases containing copies? Could there be an internal process requirement by which an insured can appeal a refusal to take action on data rights?

▪**ACTIONS NECESSARY / INSURER OBLIGATIONS TO MINIMIZE CONSUMER 'HARM':** Insurers should provide notice to consumers making them aware of their right to correct inaccurate information. Insurers should establish processes to allow for correction requests, verify that the request came from the data subject, and verify the truth of the disputed information. To the extent that the insurer declines to make the correction sought, the insurer should notify the consumer of that decision; the bases for that decision; permit the consumer to file a statement as to why the consumer disagrees with the insurer's decision; and what the consumer believes to be the correct information. The insurer should make any such statements by the consumer available to entities accessing the disputed information.

Because consumers likely are not aware of the sources from which an insurer obtains information, or entities to which the insurer provides information, the consumer is not well-suited to ensure

correction of all instances of inaccurate information. Consequently, the insurer should provide notice of corrections to any data sources or recipients.

▪**RECOMMENDATIONS:** Consumers need to be provided means for correction of inaccurate information, as those inaccuracies may have significant impacts to the insurance consumer, including cancellation or denial of coverage, or increase in fees or premium. Laws establishing the Right of Correction should require: a straightforward process by which a consumer may initiate a correction request and timely action by the request recipient; provide for verification of the identity of the requestor; provide for a dispute process governing disagreement as to the requested correction; and require notice of deletion requests to any data sources and recipients.

---

4. **TITLE OF CONSUMER RIGHT {4 above}: The Right to Delete Information**

▪**DEFINITION:** This right ensures that the underwriting process and claims adjudication will result in a fair and reasonable decision based on accurate information.

Section 9 of MDL 670 requires written request from an individual to correct, amend, or delete the portion of recorded person information in dispute. Companies still have the right to refuse to make such correction, amendment, or deletion based on lawful limitations.

The right of a data subject, after reasonable efforts by a business to verify that person's identity, to request deletion of personal information which is not necessary for the insurance transaction.

Aside from consumers' inherent interest in the privacy of their information, consumers have a compelling security interest in minimizing the amount of personal information held by other parties. Data breaches are a fact of our connected world. The right to delete allows consumers to reduce the distribution of their personal information, meaning that there are fewer opportunities for that information to be accessed or stolen by unauthorized parties.

Implementations of the Right to Delete will often specify that, upon receipt of a request for deletion and having deleted the information, the business provide notice of the deletion and a request for deletion, to third parties which either provided to the business, or received from the business, the information subject to deletion.

a. Definition – Companies must delete data upon request if the data was processed based upon the controller's legitimate interest and that interest is outweighed by the data subject's rights (GDRP).

b. Examples – A consumer of company XYZ no longer does business with XYZ. The consumer may request all data about themselves to be deleted.

▪**EXAMPLES:** NAIC Model 670,§9; Civil Code §1798.105 (CCPA); Civil Code §1798.105 (Prop. 24); Insurance Code §791.09

▪**CONSUMER RISK / IMPACT:** People have an inherent privacy interest in their personal information; the right to request deletion of that information is an essential for people to exercise control over that information. Information may grow old and outdated, to where it is no longer useful for the purpose it was collected. People may want information deleted for reasons of personal security or peace of mind (e.g.: information which relates a person to an abusive partner or spouse, or deceased loved one; information which may result in disclosure to an abusive partner or spouse). Personal information in the hands of entities other than the data subject is potentially subject to data breaches or unauthorized access; reducing the quantity of personal information "in the wild" reduces the risk of a data breach affecting the data subject.

▪**CURRENT STATE AND FEDERAL LAWS / RULES THAT APPLY (GLBA, HIPAA, 670, 672, IDSA-Insurance Data Security Model, etc.):** Ensuring patient safety and the accuracy of clinical decision-making requires a complete record of a patient's history. The record protects not only the patient but also the Covered Entity. As such, there is no specific "right to delete" in HIPAA. However, an individual's right to request that a Covered Entity correct or amend incorrect or inaccurate PHI at 45 CFR 154.526, provides a detailed process for individuals to request amendment of PHI, for Covered Entities to either approve or deny the amendment, and for the exercise of related procedural rights. In addition to the right of amendment, HIPAA provides individuals with the right of access (i.e., to inspect and receive a copy) and the right to an accounting of disclosures of PHI. While a Covered Entity must retain PHI, an individual's rights of access, amendment, and accounting provide important procedural safeguards.

In addition, state laws are replete with records-retention requirements which would, in most if not all cases, directly conflict with most interpretations of a "right to delete." Although the recent California Consumer Protection Act (CCPA) is often cited in support of the "right to delete" or the "right to be forgotten", that right is not absolute, and there are exceptions. Several of those exceptions in the CCPA are based on other regulations. For example, data already regulated by the Gramm-Leach-Bliley Act (GLBA) and HIPAA are not subject to the CCPA. However, some of the exceptions are more generally applicable and, absent further direction from the California Attorney General, open to interpretation. The exceptions apply to information necessary to complete transactions; uphold legal obligations; maintain security and existing functionality; protect free speech; conduct research; and allow for internal, expected, and lawful uses. Cal. Civ. Code Sec. 1798.105.

More information about what is intended by this right to delete information would be helpful to fully respond to this aspect of the Draft Policy Statement. Health insurers need certain PHI to perform the basic functions of the business of insurance including for treatment, payment, and health care operations. It would not be practicable to maintain a customer relationship with an individual if the individual could request deletion of his or her information. Further, federal law requires health insurers participating in federal health care programs (e.g., Medicare, Medicaid) to retain information for 10 years. Data might be required to be retained for longer periods because

of an ongoing legal action. HIPAA requires a health plan to protect member data for as long as the data is held, thus allowing consumer data to be protected over its lifespan.

We note that included in the right to correct information under HIPAA is the right to delete information that is not accurate. Additionally, an individual who has provided a specific authorization for uses and disclosures requiring authorization may revoke this authorization at any time.

Consumer Notice Requirement: The HIPAA-required Notice of Privacy Practices described in more detail above must address an individual's right to correct information held by the health insurer, which includes the right to delete inaccurate information. Individuals are informed of their right to revoke an authorization in the Notice as well.

This subject would appear to conflict with insurance laws requiring health plans to maintain records. State law and NAIC's model acts are full of requirements that health plans maintain records. The NAIC's Unfair Trade Practices Act includes at least three separate provisions that require insurers to maintain records. For example, the Unfair Trade Practices Act includes a provision entitled: ' Failure to Maintain Marketing and Performance Records'. This provision defines an unfair trade practice as the "[f]ailure of an insurer to maintain its books, records, documents and other business records in such an order that data regarding complaints, claims, rating, underwriting, and marketing are accessible and retrievable for examination by the insurance." Insurers must maintain this data for at least the current calendar year and the two preceding years. Similarly, the NAIC ' s Market Conduct Record Retention and Production Model Regulation, by its very title, requires insurers to maintain records. Under the model, insurers are generally required to retain records for at least three years i.e., insurers may not delete records during this protected period.

It also appears that HIPAA' s right to amend information, which, as noted above, health insurers are already compliant with, addresses the most obvious benefits that a right to delete information grants to an individual. If there is inaccurate information in a health file, the individual that is the subject of that information can ask that the information be corrected.

Individuals, however, should not have the right to have accurate information deleted. Health plans need this information to coordinate care, provide continuity of care and otherwise maintain information that insurance regulators might need to ensure compliance with state laws and regulations.

▪GAPS IN CURRENT STATE AND FEDERAL LAWS / RULES

▪**INSURER/LICENSEE IMPACT:** The Right of Deletion benefits insurers by reducing potential liability for data breaches or other unauthorized access, as well as reducing costs associated with the volume of information managed by the insurer. The Right of Deletion imposes administrative burdens on the insurer, including: providing processes by which the consumer may request

deletion, verification of the identity of the requestor, and determination of which data elements may be deleted without affecting provision of insurance services to the requestor.

How would the company know that the authorization is from the actual insured? What are the steps to verify that information and affirmatively identify? And what's the scope for correcting, amending, or deleting information – is the deletion from the original source or also from databases containing copies? Could there be an internal process requirement by which an insured can appeal a refusal to take action on data rights?

▪**ACTIONS NECESSARY / INSURER OBLIGATIONS TO MINIMIZE CONSUMER 'HARM':** Insurers should provide notice to consumers making them aware of their right to delete information. Insurers should establish processes to allow for deletion requests, verify that the request came from the data subject, and verify whether or not the information subject to deletion request is necessary to service the insurance policy. To the extent that the insurer declines to delete information as requested, the insurer should notify the consumer of that decision and the bases for that decision, and permit the consumer to file a statement as to why the consumer disagrees with the insurer's decision, and why the consumer believes the information is lawfully subject to deletion. The insurer should make any such statements by the consumer available to entities accessing the disputed information.

Because consumers likely are not aware of the sources from which an insurer obtains information, or entities to which the insurer provides information, the consumer is not well-suited to ensure correction of all instances of inaccurate information. Consequently, the insurer should provide notice of deletions to any data sources or recipients.

▪**RECOMMENDATIONS:** Consumers should be provided the right to instruct that personal information be deleted, provided that it is no longer necessary for completion of the insurance transaction, or for legal compliance. Laws establishing the Right of Deletion should require: a straightforward process by which a consumer may initiate a correction request and timely action by the request recipient; provide for verification of the identity of the requestor; provide for a dispute process governing disagreement as to the requested deletion; and require notice of deletion requests to any data sources and recipients. Note that HIPPA rules do not currently permit deletion requests by the consumer.

---

5. TITLE OF CONSUMER RIGHT {5 above}: The Right of Data Portability

▪**DEFINITION:** Data portability, in common understanding, is the idea of having data stored in or created in a way that is easier to transport physically or electronically from one system to another or one place to another. It facilitates the consumer's right to access their information.

This right is not defined in any of our model laws. The term portability, other than in reference to HIPAA is not being used actively. **Section 8 of MDL-670** provides for the manner of how an individual can access recorded personal information. Nothing herein describes how it can be moved from one place to another with ease. In fact, it allows insurers to have some of the information in source code, and that that they just need to translate it and provide it in writing. The consumer's right to access information is temporarily hindered by allowing information to not be readily accessible. In today's world, it is almost unthinkable for any company system be able to spit out just source codes and nothing else. Although source codes are important and regulators need them for examination, for a consumer, it will be daunting. All information used in underwriting or claim adjudication for a specific individual should be readily accessible by that individual unless certain lawful limitations exist such as those already mentioned in **MDL 670, 672, or 673**.

The right of a data subject, after reasonable efforts by a business to verify that person's identity, to request access to personal information about the data subject which is held by the business. Modern formulations of the Right of Data Portability / Access provide the data subject with the additional right to access information about how the data subject's personal information has been used or shared by the business.

a. Definition – It allows data subjects to obtain data that a data controller holds on them and to reuse it for their own purposes. Individuals are free to either store the data for personal use or to transmit it to another data controller. (GDRP).

b. Examples – A consumer of auto company XYZ is moving Their policies to company ABC. The consumer asks the XYZ, which has electronic files on them, to provide them with their personal data in a structured machine-readable format, to be able to transmit the data to ABC.

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.

The ability to obtain a copy of the consumer's personal data that the consumer previously provided to the [~~controller~~] insurer* in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another [entity/insurer*] ~~controller~~ without hindrance, where the processing is carried out by automated means.

The right to data portability allows individuals to obtain, move, copy, transfer or reuse their personal data for their own purposes across different services and/or IT environments to another one in a safe and secure way, without affecting its usability.

The data is required to be provided in a commonly used, machine-readable format.
With respect to the right of data portability, the VA Consumer Data Protection Act (VCDPA) currently provides this right to consumers covered by the VCDPA. Thus, VA Bureau of Insurance would be open to providing this right to consumers subject to GLBA. (Note: VCDPA does not apply to entities or data subject to GLBA or HIPPA.)

▪Right to data portability - You have the right to receive your personal data, which you have provided to us, in a structured, commonly used, and machine-readable format, in accordance with **Article 20 of the General Data Protection Regulation (GDPR).**

ADDITIONAL POINTS TO CONSIDER:

▪Address Personally Identifiable Information-PII and Personal Health Information-PHI; applies to HIPAA or not?

▪Article - https://searchcloudcomputing.techtarget.com/definition/data-portability

▪Federal Medicare/Medicaid rule pertaining to **Electronic Health Record-EHR**: An electronic health record is the systematized collection of patient and population electronically stored health information in a digital format. These records can be shared across different health care settings. An **Electronic Medical Record-EMR** is best understood as **a digital version of a patient's chart**. It contains the patient's medical and treatment history from one practice. By contrast, an **EHR contains the patient's records from multiple doctors** and provides a more holistic, long-term

view of a patient's health. Electronic Health Records (EHR s) are the first step to transformed health care. The benefits of electronic health records include better health care by improving all aspects of patient care, including safety, effectiveness, patient-centeredness, communication, education, timeliness, efficiency, and equity.

Where can I get answers to my privacy and security questions about electronic health records (EHRs)? The Office for Civil Rights (OCR) is responsible for enforcing the Privacy and Security rules related to the HITECH program. More information is available at OCR's website at http://www.hhs.gov/ocr/index.html or ONC's website at https://www.healthit.gov/topic/privacey-security-and-hipaa.

▪**EXAMPLES:** NAIC Model 670,§8; Civil Code §§1798.100, 1798.110, 1798.115 (CCPA); Civil Code §§1798.100, 1798.110, 1798.115 (Prop. 24); Insurance Code §791.08

▪**CONSUMER RISK / IMPACT:** People have an inherent privacy interest in information about them; an important aspect of that right is the ability to access personal information which businesses hold about the person. Consumers cannot make meaningful choices with respect to their information privacy, without access to the information which businesses hold about the consumer. Access is essential to allow the consumer to verify that businesses are complying with legal obligations under data privacy laws, and that data held about the consumer is accurate.

▪**CURRENT STATE AND FEDERAL LAWS / RULES THAT APPLY (GLBA, HIPAA, 670, 672, IDSA-Insurance Data Security Model, etc.):** The Federal privacy statutory and regulatory framework handles portability in two main ways. First, the HIPAA Privacy Rule provides individuals with the right to access and obtain a copy of the protected health information about the individual (45 CFR 164.524). Additionally, an individual has the right to receive an accounting of all disclosures of their information made by a covered entity within the previous six years (45 CFR 164.528). An individual can also direct disclosures to third parties (e.g. an attorney in a civil suit) by signing a written authorization for the specific information and the individual or entity to whom the protected health information should be disclosed. See 45 CFR 164.524(cc)(3)(ii). Earlier this year, HHS issued a notice of proposed rulemaking which would further strengthen an individual's right of access and the right to direct disclosure of PHI to third parties. See 86 FR 6446 (January 21, 2021).

Second, the recent 2020 Interoperability and Patient Access final rule was intended to innovate and streamline how consumers access their medical records from their health insurers in federal programs. The regulation requires the development and use of application programming interfaces (APIs) to seamlessly share electronically protected health information with third-party applications or "apps" for consumers to access their health information to improve their health, monitor their conditions, or other related services. However, we note that this process moves the personally

identifiable information outside the reach of HIPAA, potentially leaving the patient's information vulnerable.

There are a few ways in which an individual can obtain and reuse/repurpose his or her information under existing and rapidly evolving federal law. First, under HIPAA, an individual has a right of access to inspect and obtain a copy of PHI about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set. A health insurer must provide the individual with access to the PHI in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual.

Pending federal regulations would further expand the HIPAA-required right of access. The proposed regulations would expressly prohibit a covered entity from imposing unreasonable measures that would impede an individual's right of access. It would also create a separate set of provisions addressing an individual invoking their right to direct electronic copies of PHI, if maintained in an electronic health record, to a third party as required by the HITECH Act.

In addition, beginning on July 1, 2021, certain insured consumers will have near real-time access to certain data pursuant to the Centers for Medicare and Medicaid Services (CMS) interoperability requirements. Medicare Advantage plans, Medicaid managed care organizations, and qualified health plan issuers participating in the Federally facilitated Exchanges must provide a secure FHIR-based application programming interface (API) available to third-party apps and developers. At the direction of the enrollee, the impacted payers must allow access to this Patient Access API within one business day. The API must include a minimum set of data:

- Adjudicated claims and cost information
- Provider remittances
- Cost-sharing
- Clinical data as defined in USCDI v1 if maintained by the payer
- For Medicare Advantage plans with Part D coverage, they must make available formulary and prescription drugs.
- For Medicaid managed care organizations, they must make available preferred drug lists.

Note that beginning in 2022, a separate requirement under the CMS interoperability rules requires impacted payers to exchange, at a minimum, the USCDI elements, at a patient's request, with another payer. The receiving payer must incorporate into the plan's records, thus creating a more longitudinal record for the individual regardless of his or her plan.

Consumer Notice Requirement: The HIPAA-required Notice of Privacy Practices described in more detail above must address an individual's right to inspect and obtain a copy of PHI held by the health insurer.

Portability, as the term is used in the GDPR and the CCPA, is inappropriate for application to the health insurance industry. These laws define portability as the ability of an individual (data subject) to receive the personal data the individual has provided to a controller and transmit it to another controller without hindrance from the controller that presently has the data. At the heart of this concept is that individuals should be allowed to freely move their own data from one controller (insurer) to another controller (presumably any other business entity that collects data) whenever they want to move the data. As we noted in previous comments, the health insurance industry is not the target of either the GDPR or the CCPA. Rather, their focus is the service and technology industries that collect, compile, and sell consumer information. Rules aimed at Google, Microsoft, Amazon, or other large technology companies are not necessarily appropriate for the health insurance industry, and in this case, they clearly are not.

The 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 can be held hostage by the controllers that are in possession of the individual's information so that, for example, an individual would not be able to select a new telephone service provider until the former releases the number, and once the individual has selected a new service provider, the former provider no longer needs the consumer's data. This potential harm does not exist in the health insurance industry. Health insurers do not control their customers by maintaining their health records. Employers and individuals regularly switch insurers, and individuals have the right to freely authorize and direct their information be given to another insurer.

As discussed above regarding the right to delete information, portability rights, if coupled with a deletion requirement, would also appear to conflict with state insurance laws requiring health plans to maintain accurate and complete records. If an individual could direct a health insurer to transmit the individual health and insurance information to another controller without hindrance, and then direct the insurer to delete the information transmitted, it would be impossible for the health insurer to maintain information as required by state law, it would jeopardize continuity of care and would make the maintenance of accurate health records difficult, if not impossible. It also has the potential to make it impossible for state insurance regulators to conduct their market conduct and examination functions if health plans are unable to maintain the records of their policy and certificate holders.

▪GAPS IN CURRENT STATE AND FEDERAL LAWS / RULES:

▪**INSURER/LICENSEE IMPACT:** The Right of Data Portability / Access benefits insurers by allowing the consumer the opportunity to verify the accuracy of information held by the insurer. The Right of Data Portability / Access imposes administrative burdens on the insurer, including: providing processes by which the consumer may request access, verification of the identity of the requestor, and provision of the requested data elements in a format readily accessible by the requestor.

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 can 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.

The ability for Data Portability to:

- Pull info from consumer section above, good info in article from Becker's Healthcare
- Check requirements from IT Handbook; data transfer guidance {new WG drafting standards}

▪ACTIONS NECESSARY / INSURER OBLIGATIONS TO MINIMIZE CONSUMER 'HARM':

▪**RECOMMENDATIONS:** Insurers should provide notice to consumers making them aware of their right to access. Insurers should establish processes to allow for access requests, verify that the request came from the data subject, and provide the requested information in a format readily usable by the consumer. To the extent that the insurer declines to provide access, the insurer should notify the consumer of that decision, the basis for that decision, and provide for a dispute process.

Insurer "Good Faith / Professional Judgment" Safe Harbor for disclosures pursuant to requests for access?

Cross with the right to restrict the use of data

Right to Data Portability [Troutman paper]

The CCPA gives consumers the right to obtain a copy of their personal information "in a readily useable format that allows the consumer to transmit [the] information from one entity to another entity without hindrance." In effect, this requirement gives consumers a data portability right, since they can migrate their personal information from one business to another offering similar services. This right was modified by the CPRA to require businesses to provide copies of the personal information obtained from the consumer "in a format that is easily understandable to the average consumer, and to the extent technically feasible, in a structured, commonly used, machine-readable format, which also may be transmitted to another entity at the consumer's request without hindrance."

The CDPA provides a more limited right to data portability. First, the CDPA only requires that the controller provide a portable copy of the personal data "that the consumer previously provided to the controller," not all the data that was collected concerning the consumer. Second, the requirement that, to the extent technically feasible, the data be provided in a readily useable format that allows the consumer to transmit the data to another controller without hindrance is limited by the provision that such format is only required "where the processing is carried out by automated means." The phrase "where the processing is carried out by automated means" is also not defined or further explained. The CDPA; however, defines processing as "any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage disclosure, analysis, deletion or modification of personal data." By adding the plain meaning of automated (not requiring human intervention), the phrase may limit a consumer's right to receive a portable and readily usable copy of the data solely to data that is processed without human intervention.

---

6. TITLE OF CONSUMER RIGHT {6 above}: The Right to Restrict the Use of Data

▪**DEFINITION:** The right of the data subject to limit use of their personal information to certain uses specified by the consumer. As implemented in Prop. 24, the right is formulated as the right to limit use or disclosure of personal information.

In effect, this is an enhancement on the rights to opt-out/opt-in; consumers may opt-out/opt-in of use of their personal information for certain purposes.

The right to opt in and out of data sharing has the implied right to restrict the use of data.

Section 13 of MDL 670 enumerated the instances where sharing/disclosure is allowed that in effect, restricts the use of data reasonably.

a. Definition – An individual can limit the way that an organization uses their data. This is an alternative to requesting the erasure of their data. Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction.

b. Examples – A company may only collect, access, use, maintain, or disclose Privacy Restricted Data to fulfill its obligations under this Agreement.

▪**EXAMPLES:** Civil Code §1798.121 (Prop. 24)

▪**CONSUMER RISK / IMPACT:** The Right to Restrict Use of Data allows consumers control over how insurers use their information. Rather than a blanket opt-out or opt-in, a Right to Restrict Use permits the consumer to tailor how insurers use the consumer's information, consistent with the consumer's preferences.

▪**CURRENT STATE AND FEDERAL LAWS / RULES THAT APPLY (GLBA, HIPAA, 670, 672, IDSA-Insurance Data Security Model, etc.):** The HIPAA Privacy Rule provides individuals with the right to request a covered entity to restrict uses or disclosures of their information to carry out treatment, payment, or health care operations, as well as other otherwise permitted disclosures. See 45 CFR 164.522. There are also provisions within HIPAA for "confidential communications" which set out processes for agreed-upon information disclosures.
Health insurers address an individual's right under HIPAA to restrict the use of data as authorized in 45 C.F.R. §164.522(a) in the sections above regarding "opt-out" and "opt-in" rights. However, we welcome additional clarity from the Working Group regarding any distinctions intended among these rights.

Consumer Notice Requirement: Similarly, health insurers address consumer notice regarding an individual's right to restrict the use of data above.

Health plans are already subject to the HIPAA privacy rule requirements granting individuals the right to request restrictions regarding the use and disclosure of their protected health information for treatment, payment and operations and the right of individuals to request restrictions for other disclosures, such as those made to family members. We, therefore, urge an exemption for health plans that already are HIPAA compliant.

▪GAPS IN CURRENT STATE AND FEDERAL LAWS / RULES

▪**INSURER/LICENSEE IMPACT:** Much like the Rights to Opt-Out/Opt-In, the Right to Restrict Use imposes administrative burdens on insurers, consistent with providing notice of the right, a process for consumers to state their preferences, and administering personal information use and disclosure consistent with the preferences of the consumer.

▪ACTIONS NECESSARY / INSURER OBLIGATIONS TO MINIMIZE CONSUMER 'HARM'

▪RECOMMENDATIONS

ADDITIONAL CONSIDERATIONS FOR DISCUSSION: Consumer perspective: Common themes that resonate with consumers include the need for stronger protections (collect less data, better stewardship of data collected, opt-in not opt-out); more consumer control (Right to correct and delete data, Right to restrict use); greater transparency about company privacy policies; expanding definitions of "personal data"; expansion to include automated decision making; provision of consumer redress for privacy violations; and a dedicated data protection agency. Another consumer perspective is that consumers should not have the primary responsibility in privacy protections because many consumers underestimate the scope and depth of personal information collected about them; and there is no easy way for consumers to control industry data collection and management. So, regulators and industry should have the primary roles, but consumers should still have data privacy rights.

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, the Working Group 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.

How workable is this model for compliance? Should there be other exemptions? Are there any additional protections for vulnerable (elderly, etc.) persons? Should new types of data such as telematics be expressly included in the definition of "personal information?" How do these privacy standards overlap with market conduct examinations?

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.

HIPAA regulates the health insurance industry as well as the broader health care system. Health insurers have spent years implementing and maintaining compliance with these and other HIPAA-mandated national requirements to ensure their consumers' privacy rights are well-protected. Further, this is a system that is regularly reviewed and improved (e.g., HITECH, and the Interoperability Rule). Health insurers urge the Privacy Protections Working Group to preserve

these exemptions for insurers subject to HIPAA by avoiding any action that conflicts, challenges, or needlessly duplicates these requirements.

1. In addition to identifying substantive minimum consumer data privacy protections as is currently laid out in the Draft Policy Statement, the framework should narrow its applicability to specifically exempt health insurers through a "carve-out" provision. Health insurers are already subject to extensive and evolving data privacy protection requirements under the Health Insurance Portability and Accountability Act (HIPAA) and other federal laws.

2. To the extent that health insurers already subject to HIPAA are not exempt from all privacy protections developed to be incorporated into NAIC model #672, the model, with respect to health insurers, should conform to HIPAA standards so that consumers remain protected without creating duplicative, confusing, and burdensome requirements that add potentially little to no additional consumer protection.

CONCLUSION:

After review of state privacy laws, NAIC Model 672 and 670, and considering the rapid changes in technology (apps and trackers) and how easy it is to get information from and for almost everything, the Working Group recommends including: 1) proper disclosures that state clearly all information collected and source of information; then, make this readily available for when a consumer requests it; and 2) disclose why this information is gathered. MDL-672 and MDL-670 have some language that pertains to this, but it needs to be updated to encompass the broader ability of insurance companies and their producers to obtain information about the insured, the insured's properties, or its beneficiaries. Because different states (and countries) have taken different approaches to consumer data privacy issues, all items listed in this policy statement, for both consumer notice rights and the subjection of insurers to those rights, should be included.

The most efficient way to resolve the data risks for consumers via regulation is to update **MDL 670, 672, and 673** instead of creating a whole new model act. However, these acts may need to be repackaged for some other states whose legislators need a little bit more comfort that this is not business control but freedom of information to people who own the personal and privileged information.

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.

W:\National Meetings\2021\Fall\Cmte\D\Privacy Protections\Aug 30 Call\First Working Group Exposure Draft Of Privacy Policy Statement_082621.Docx

