Comments On Insurance Consumer Privacy Protection Model Law #674 Exposure Draft
Submitted to the Privacy Protections (H) Working Group

Harold Ting, PhD
NAIC Consumer Representative
March 7, 2023

My name is Harold Ting. I am an NAIC Consumer Representative, and I am submitting these comments as an ordinary citizen, drawing on my personal experience and my experience as a SHIP counselor in Pennsylvania, where I have counseled over 400 insurance consumers who qualify for Medicare because of disability or age.

Since getting involved with the Privacy Protection Work Group two and a half years ago, I have become more aware of how the personal information of individuals can be captured and misused. Now whenever I go to a new website, I try to open the link to its privacy policy and minimize the data that it can retain and utilize in ways unknown to me. Sometimes I have to read the policy to find where I can exercise that option. But at times, it takes too much time and effort, and sometimes I get no choice, if I want to use that website. So I acquiesce somewhat unwillingly.

There have been several times, where someone has captured my credit card information and charged using it, forcing me to change my card number. I am frustrated that my online searches lead to so many vendor emails peddling products or services, that emails that I want to see get lost in them. Worst of all, with increasing frequency, I am getting phishing emails and texts disguised as messages from companies I use, trying to steal my personal information. In addition I cannot escape sharing personal information that I have no desire to share, because it is shared by my phone, my tv, my car and my appliances through the Internet of Things.

In this environment, I wish the federal government would take measures to provide greater protection of my personal information. But lobbying by companies like Google and Meta is making it difficult for that to happen, because their business models are based upon capturing data about me. In this context, NAIC has an opportunity to advance privacy protection measures that are never going to be enacted for all industries. It is timely to pass fair consumer privacy measures for the insurance industry, because the business model of key players in the industry is not yet based on sharing or selling consumer data.

In this context, I am very pleased to see that the Exposure Draft of Model Law #674 establishes clear standards for protecting consumer privacy in the areas of:

- transparency– sharing an organization's privacy policy and protecting consumer privacy at the time of collection;
- data minimization –limiting information collected to only data needed for requested insurance transactions;

- use limitation –prohibiting selling or sharing personal information for other purposes unless permission is given explicitly;
- ability to review and correct – allowing consumers to review and correct personal information that was collected, or to add documentation to their record, where they dispute its accuracy;
- requiring third party service providers to meet the same privacy standards through written agreements;
- accountability – establishing penalties to incent licensees and their third-party service providers to comply with the Model Act.

Recognizing that it is unlikely that all states and territories will adopt this Model essentially as written, I would hope that insurance licensees will adopt the practices it requires anyway. Where they do, they are likely to meet any other consumer privacy protection requirements that exist in the states where they operate.

In the remainder of these comments, I present six reasons I believe the requirements in the Exposure Draft are needed and recommend a few areas where I think the Model can be improved.

Why The Requirements of the Exposure Draft Are Needed

1. Saying Consumers Aren't Complaining is NOT A Valid Reason to Keep the Status Quo

Claims that consumers are not complaining about abuses of the personal information that licensees and their third-party service providers (TPSP's) collect totally misses the point. Currently consumers don't have any way to know how their information is shared and used. So in most cases, they have no way to attribute harm caused by information sharing of licensees and TPSP's.

2. Privacy Protection Must Be the Default of Privacy Policies

Privacy protection policies should always default to non-disclosure of personal information. It is well documented that most consumers do not read entire corporate privacy policies. It is neither realistic to expect consumers to do so, nor to expect that they can fully understand what is in them. Privacy policies are too long and complex. Moreover, some companies use dark patterns that manipulate consumers into permitting greater use of their personal data than they desire.[1]

3. Restrictions Similar to Those Imposed by HIPAA Are Needed

In NAIC's January 2001 FAQ document on Model Regulation #672, it stated *"The health rules differ from the financial rules, because state financial regulators believe your health information is more*

[1] From *Dark Patterns Cannot Stay in the Dark*, by S. Jeong, M. Sturtevant and K. Stephen, The Regulatory Review, 2022 (https://www.theregreview.org/2022/05/28/saturday-seminar-dark-patterns-cannot-stay-in-the-dark/).

sensitive than financial information and need greater protections. That is why there is an affirmative consent requirement ('opt-in') for health information as opposed to the 'opt out' requirement for financial information."[2] In 2023, with the fraudulent use of the financial data of millions of people, the threat of personal harm when individuals' sensitive information is spread about them, and other common misuses of personal information, non-health personal information clearly needs equal protection. The general privacy protections that make sense for personal health information should be applied to all personal information collected by all licensees.

4. For Model #674 to Be Effective, Third Party Service Providers to the Same Standards As Licensees

Given the extensive use of TPSP's in the collection and processing of consumers' personal information, it goes without saying that licensee privacy standards will only be effective if TPSP's adhere to them as well. Because state insurance departments generally do not have authority to regulate TPSP's, requiring TPSP's to follow the same standards is the only way that can be done. Not doing so would leave a huge loophole that would eviscerate the privacy protection of Model #674.

5. Data Minimization Is Essential Because It Is Impossible to Totally Prevent Data Breaches

According to the Identity Theft Resource Center, 1774 data breaches in the U.S. were reported publicly in 2022. These affected 392 million "victims". The top 10 data items breached included information on medical history/condition/treatment/diagnosis, health insurance account number and medical provider information.[3]

Over the last five years insurance companies as diverse as Anthem, Prudential Financial, John Hancock, Allstate, and State Farm have each reported multiple data breaches.[4] Major third-party service provider breaches last year included ones by Shields Health Care Group, a medical imaging company, Professional Finance Company, a debt collection company, and Verisk Analytics, one of the world's largest insurance data aggregators.[5,6] One of the largest such breaches involved debt collection company American Medical Collection Agency, where data on over 20 million people

---

[2] From *NAIC Privacy of Consumer Financial and Health Information Model Regulation: Frequently Asked Questions*, 2001, p. 8 (https://naic.soutronglobal.net/Portal/Public/en-GB/DownloadImageFile.ashx?objectId=6471&ownerType=0&ownerId=5475)

[3] From *2022 Data Breach Report*, Identity Theft Resource Center, January 2023.

[4] From Identity Theft Resource Center (https://www.idtheftcenter.org/notified).

[5] From *1.9M Patient Records Exposed in Healthcare Debt Collector Ransomware Attack*, by J.R. Hardcastle, TechCrunch, 2022 (https://techcrunch.com/2022/07/13/pfc-ransomware-healthcare/).

[6] From ClassAction.org (https://www.classaction.org/news/verisk-analytics-data-breach-exposed-millions-ofconsumers-private-information-class-action-alleges).

was stolen in 2019. After the company was fined $21 million by 41 state attorney general, AMCA filed for bankruptcy.[7]

The data minimization requirement in Model #674 was fully supported by the Electronic Privacy Information Center's statement to the U.S. House of Representatives last month. In it, EPIC stated the "baseline requirement that companies must limit their data collection to what is reasonably necessary and proportionate 'to provide or maintain a product or service requested by the individual' .... is the standard that the Committee on Financial Services should be imposing on entities subject to the GLBA."[8]

6. Compliance Is Key

Model Law #674 will only be effective if there are meaningful penalties for non-compliance. There is no practical way that state insurance departments can adequately monitor compliance of thousands of licensees and TPSPs. To be effective, regulators must have the ability to wage meaningful penalties where serious violations occur, so companies will not want to risk being caught breaking the rules.

Recommended Revisions

1. Article III, Section 7.A Should Also Require Disclosure of Consumer Reporting Agencies Used

To the extent that licensees or TPSP's collect information from consumer reporting agencies, such as data brokers, those sources should also be disclosed. That is relevant, because the accuracy of data supplied by such sources is more likely to be suspect. For example, cookie and website tracking tools that showed I was looking online for cancer treatments or auto collision body shops could impact health or auto insurance underwriting for me, even if I did those searches for a friend. A 2019 study published by the Academy of Computing Machinery found at least 40 percent of data broker sourced user attributes were not at all accurate.[9] Attachment A to these comments adds consumer reporting agencies to the sources required to be disclosed, so consumers can decide whether they want to check the accuracy of their data collected by consumer reporting agencies.

---

[7] From *41 States Settle with AMCA Over 2019 Data Breach Affecting 21M Patients*, by J. Davis, Health IT Security, March 12, 2021 (https://www.healthitsecurity.com/news/41-states-settle-with-amca-over-2019-data-breach-affecting-21m-patients).

[8] From Epic Statement to the U.S. House of Representatives Committee on Financial Services re: Data Privacy Act of 2023, February 27, 2023 (https://epic.org/documents/epic-statement-re-data-privacy-act-of-2023/).

[9] From *Auditing Offline Data Brokers via Facebook's Advertising Platform* by G. Venktadri, P. Sapiezynski, E. Redmiles et.al., WWW'19: The World Wide Web Conference, 2019 (https://doi.org/10.1145/3308558.3313666).

2. Article V, Section 14 Should Be Revised and Not Be Optional

Section 14 of Article V protects the ability of consumers to obtain reasons for adverse underwriting decisions. Under Subsection A a licensee responsible for such a decision does not have to include the reasons for such a decision in its notification to the consumer. The Subsection allows the licensee to require the affected consumer to submit a written request to obtain those reasons. That is totally unreasonable. Consumers should be given the reasons immediately, so that they can either contest the adverse decision or seek an alternative insurance transaction. Under Subsection B, it could take at least 10 business days plus the time to transmit written notification of an adverse decision and the time to transmit a request the reasons – unnecessary and unjustifiable delay. Suggested revised wording follows these comments in Attachment B.

3. Data Security and Privacy Are Inextricably Connected: Add Provisions Regarding Data Security

As noted earlier in these comments, serious data breaches of personal information collected by licensees and TPSP's occur in the insurance industry. To minimize such occurrences, it is critical that those parties adopt effective data security procedures and practices. Requirements to establish reasonable data security procedures and practices are included in the California Consumer Privacy Act and the California Privacy Rights Act, the Colorado Privacy Act, and the Virginia Consumer Data Protection Act. Model Act #674 should have such provisions too.

There are other NAIC models that include sections regarding data security. The most recent and comprehensive model is Insurance Data Security Model Law #668, which was adopted by NAIC in 2017. However, as of last fall, 30 states and territories had not adopted Model Law #668 or similar requirements in some form.[10] Model Law #674 should either incorporate Model Law #668 provisions or establish other minimum data security requirements that licensees and third-party service providers must meet.

[10] From *Insurance Data Security Model Law ST-668-1,* NAIC Model Laws, Regulations, Guidelines and Other Resources — Fall 2022 (https://content.naic.org/sites/default/files/model-law-state-page-668.pdf)

ATTACHMENT A
SUGGESTED ARTICLE III, SECTION 7, SUBSECTION A REVISION

(*revised wording is in italics & underlined*)

Section 7. Content of Consumer Information Practices Notices

A. The content of any notice required by Section 6 shall state in writing all of the following:

(1) Whether personal information has been or may be collected from any sources other than the consumer or consumers proposed for coverage, and whether such information is collected by the licensee or by a third-party service provider *or by consumer reporting agencies*;

(2) The specific types of personal information of the consumer that the licensee or any of its third-party service providers *or consumer reporting agencies* has or may collect, process, retain, or share;

ATTACHMENT B
SUGGESTED ARTICLE V, SECTION 14 REVISION

ARTICLE V. ADVERSE UNDERWRITING DECISIONS; OTHER TRANSACTIONS

Section 14. Adverse Underwriting Decisions

A. Notice of an adverse underwriting decision. In the event of an adverse underwriting decision the licensee responsible for the decision shall provide in writing to the consumer at the consumer's address of record:

(1) The specific reason or reasons for the adverse underwriting decision, provided;

(a) A licensee shall not be required to furnish specific privileged information if it has a reasonable suspicion, based upon specific information available for review by the Commissioner, that the consumer has engaged in criminal activity, fraud, material misrepresentation or material nondisclosure, or

(b) Health information supplied by a health care provider shall be disclosed either directly to the consumer about whom the information relates or to a health care provider designated by the individual consumer and licensed to provide health care with respect to the condition to which the information relates,

(2) A summary of the rights established under Subsection C and Sections 11 and 12 of this Act; and

(3) The names and addresses of the sources that supplied the information outlined in Subsection A(1); provided, however, that the identity of any health care provider shall be disclosed either directly to the consumer or to the health care provider designated by the consumer.

B. The obligations imposed by this section upon a licensee may be satisfied by another licensee authorized to act on its behalf.