Arbor Strategies, LLC

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

September 9, 2021

Ms. Cynthia Amann
Chair, NAIC Privacy Protections (D) Working Group
Missouri Department of Insurance
301 W High St Rm 530
Jefferson City, MO 65101

Dear Ms. Amann:

I am writing on behalf of a Coalition[1] of health insurers representing some of the country's largest major medical insurers and health maintenance organizations to comment on the NAIC Privacy Protections (D) Working Group's ("Working Group") proposed FIRST WORKING GROUP EXPOSURE DRAFT OF PRIVACY POLICY STATEMENT dated August 30, 2021 ("Exposure Draft") We offer the following comments in the hopes that our comments will provide additional focus to the Working Group's discussion in order to streamline the Exposure Draft with the goal of having the document available for the December national meeting.

Need for a Specific Definition

In our June 7, 2021 letter (and in earlier comments), the Coalition requested a better understanding of what the Working Group intended by the "right" to "opt out of data sharing." We noted a need for clarity about what that term actually entails before there can be a meaningful discussion on this issue. Unfortunately, the definition found in the Exposure Draft does not provide the necessary clarity. The Exposure Draft provides the following definition

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

of 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."[2]

This definition does not appear to address the specifics of opting out of data sharing. It is actually a broad policy, or aspirational statement, but not a defined legal term. As drafted, the term is so broad that the statement could apply to almost all of the rights enumerated in the Exposure Draft. For example, the "right to restrict the use of data" is very much related to the "ability of consumers to retain control of what data can be shared and with whom." This equally applies to the "right to opt in of data sharing", i.e., insures may not share a consumer's data unless the consumer opts into the sharing of the data. But as written, the current term does not provide sufficient legal guidance upon which stakeholders can rely.

The Exposure Draft should include a specific legal definition of the right to opt out. By doing so, the Working Group and interested parties can have a direct and meaningful discussion as to whether the NAIC should include this definition in future models, guidance, or other discussion papers. We recommend that the Exposure Draft adopt the definition in NAIC Model 672. Model 672 defines the right to opt out as follows: "opt out means a direction by the consumer that the licensee not disclose nonpublic personal financial information about that consumer to a nonaffiliated third party, other than as otherwise permitted by law."[3] This is the most common usage of the term among the industry. It is also the most common usage of the term as it is presented to consumers. When consumers receive opt out notices with the privacy statements that they receive from insurers, it is the Model 672 definition of this right that those notices are referencing. To change that definition at this point would cause significant confusion.

By using this specific definition, the Working Group can begin the discussion as to whether the right to opt out should remain in the future NAIC privacy models. This definition could also prompt additional discussion as whether disclosures for marketing purposes are appropriate, what exceptions to the right to opt out should remain in law, whether they should be expanded/contracted as well as discussion on other issues that fall under this definition.

---

[2] Exposure Draft at page 6.
[3] Model 672 at §12.A.(2).

Recommendations are Overly Broad

We are also concerned with the recommendations put forth in the Exposure Draft. The Exposure Draft contains the following recommendation: "RECOMMENDATIONS: Consumers should be afforded a comprehensive right to control the use of their personal information for purposes unrelated to the insurance transaction."[4] We believe that this recommendation goes beyond the actual protections afforded to consumers and could actually mislead consumers as to their actual rights. For example, the right to opt out is not comprehensive. There are necessary exceptions recognized in Model 672 to the right to opt out of data sharing that go beyond insurance transactions. First, consumers may only opt-out of disclosures to nonaffiliated third parties. The other exceptions are 1) to opt out of requirements for disclosure of nonpublic personal financial information for service providers and joint marketing; 2) to opt out of receiving notices regarding disclosure of nonpublic personal financial information for processing and servicing transactions; 3) to opt out of other exceptions to notice and other requirements for disclosure of nonpublic personal financial information.[5]

More generally, all privacy laws recognize that insurers may use and disclose information for purposes of conducting the business of insurance. To allow consumers to opt out of these kinds of disclosures would run contrary to state law and would likely be preempted by HIPAA privacy rules. State and federal law also require insures to make certain types of disclosures, i.e., to state regulators, to law enforcement, etc. Consumers may not opt out of these types of disclosures. To suggest that consumers have a comprehensive right to control their data is not accurate and a statement of this type should not be included in the recommendations.

Rather the recommendations should focus on a specific definition of opt out. The discussion should address whether this right should be retained, expanded or limited. By focusing the discussion, we can reach useful conclusions.

General Observations

Changes to the privacy rules must be done cautiously and carefully. The United States Department of Health and Human Services ("HHS") recently published comments that share our

[4] Exposure Draft at page 25.
[5] Model 672, §§ 15, 16 & 17.

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."[6] HHS also warns that the unintended consequences of privacy rules that fail to consider all of 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."[7]

Any new model should include a HIPAA safe harbor. 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."[8]

The rules that apply to technology companies are not appropriate for the health insurers. The GDPR and the CCPA frameworks are inappropriate for application to the health insurance industry. Key to these laws is 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.

Federal Register, Vol. 86, No. 12, Thursday, January 21, 2021 at page 6447.

[7] *Id.* at page 6447.
[8] Model 672, §21

Thank you for the ability to comment. If you have any questions, please feel free to reach out to me at either (202) 247-0316 or cpetersen@arborstrategies.com. We look forward to working with the Working Group as it discusses topics for possible inclusion in a revised NAIC privacy model.

Sincerely,

Chris Petersen

cc: Lois Alexander