CARLTON FIELDS

NAIC's New Privacy Protections Recipe

May 25, 2023

In April and May, the NAIC Privacy Protections Working Group held the first three of its biweekly calls to discuss its recipe for a new privacy model, "Insurance Consumer Privacy Protection Model Law #674." During the meetings, the working group considered whether the recipe needed to (a) include, as an ingredient, a private right of action; (b) clarify the HIPAA safe harbor; (c) leave more or less room for "secret sauce" (i.e., revise its confidentiality provisions); (d) revisit its kitchen cleanup processes (i.e., data retention and destruction requirements); and (e) locally source its ingredients (i.e., restrict cross-border data transfers).

Private Right of Action

The debate on whether to include a private right of action within the privacy model was similar to deciding whether a recipe should include cilantro — some love it, while for others it leaves a soapy aftertaste. As expected, consumer advocates sought to preserve a private right of action. They asserted that eliminating it would deprive consumers of any redress for the unwanted use of their personal information and make noncompliance a mere cost of doing business. The advocates alleged that this additional ingredient was necessary to counter insurers' increased data use and "surveillance economy," as regulators would not have the resources to enforce the draft model's protections. Those against its inclusion countered that the ingredient merely preserves the status quo; removing the language does not take away any existing causes of action.

HIPAA Safe Harbor

Discussions on the HIPAA safe harbor were less divisive. The commentators generally agreed that the recipe should include a HIPAA safe harbor. The question was how much to add and how to express that in the recipe (i.e., for the HIPAA safe harbor to apply, is it sufficient for entities to be subject to HIPAA or subject to and in compliance with HIPAA? And how should that apply to entities with varying lines of business, some of which are subject to HIPAA and others that are not?).

Confidentiality Provisions

Industry and consumer advocates debated the extent to which the model's recipe should protect secret sauce. Industry advocates requested that the optional contractual provisions between regulators and their contractors be made mandatory and expanded to protect all confidential data provided to regulators, even if not a part of a market conduct exam, stressing the importance of such protection to protect service providers' intellectual property. Consumer advocates, however, said that existing law provided sufficient confidentiality and that the model should not include any confidentiality provisions but rather require additional reporting and disclosures to help consumers "discipline insurers."

Document Retention and Deletion

Industry and consumer advocates also split on kitchen cleanup (i.e., the model's data retention and destruction provisions). Industry advocates explained that requiring deletion within 90 days of no longer needing personal information was a technical impossibility for legacy systems and would require years to implement, that individual confirmation of document deletion was unworkable, and that a risk-based (rather than the current one-size-fits-all 90-day proposal) was necessary. Regulators expressed openness to step up compliance or extended implementation deadlines and requested industry input regarding how long would be needed. Consumer advocates, however, requested the draft model be revised to lessen insurer discretion regarding the amount of time for which personal information would be retained. Regulators explained that their data minimization concerns were due to the risk of data breaches and that they were entirely unconcerned with de-identified data, with one regulator exclaiming: "If you can de-identify it, then go ahead and keep it forever."

Cross-Border Data Transfers

Consumer advocates appeared ambivalent as to whether their ingredients were locally sourced, but industry advocates raised sharp concerns over the draft model's proposal to require consent for all cross-border transfers, stating that such a requirement:

- Might offend, or be preempted by, international treaties;
- Is contrary to the increasingly global nature of business and is unduly burdensome for companies with global operations;
- Would exceed the protections put in place by state privacy laws; and
- Would harm consumers by increasing costs and decreasing the availability of 24-hour customer service without improving either security or consumer control over their data.

Instead, industry commentators encouraged the working group to explore vendor oversight and required contractual provisions when transferring data to service providers or vendors abroad (e.g., requiring international data processors to commit to certain cybersecurity practices and regular oversight and submit to the jurisdiction of U.S. regulators).

Next Steps

The working group made no final decisions but expressed its expectation to revise its recipe based on the feedback received. Next, the working group has invited regulators and other interested parties into the test kitchen for two full days of recipe development on June 5–6. Get your taste buds ready!

Authored By

Ann Young Black

Patricia M. Carreiro

Related Practices

Cybersecurity and Privacy
Financial Services Regulatory
Life, Annuity, and Retirement Solutions

Related Industries

Life, Annuity, and Retirement Solutions
Life, Annuity, and Retirement Solutions

link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.