

Draft: 5/4/23

Privacy Protections (H) Working Group
Virtual Meeting
April 18, 2023

The Privacy Protections (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met April 18, 2023. The following Working Group members participated: Katie Johnson, Chair (VA); Cynthia Amann, Co-Vice Chair (MO); Chris Aufenthie, Co-Vice Chair (ND); Chelsy Maller (AK); Gio Espinosa and Catherine O'Neil (AZ); Damon Diederich (CA); C.J. Metcalf and Erica Weyhenmeyer (IL); LeAnn Crow (KS); Ron Kreiter (KY); Alexander Borkowski and Van Dorsey (MD); Jeff Hayden (MI); Santana Edison (ND); Teresa Green (OK); Gary Jones (PA); Patrick Smock (RI); and Todd Dixon (WA). Also participating was Doug Ommen (IA).

1. Discussed Private Right of Action (Section 28—Individual Remedies)

Johnson said the Working Group would be discussing the use of the following private right of action wording from the *Insurance Data Security Model Law* (#668) in place of the wording in Section 28(A) and (B) in the new *Insurance Consumer Privacy Protection Model Law* (#674):

This Act may not be construed to create or imply a private cause of action for violation of its provisions, nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.

Shelby Schoensee (American Property Casualty Insurance Association—APCIA) said the APCIA would be okay with the wording, as it is better than that in the original Feb. 1 exposure draft. Bob Ridgeway (America's Health Insurance Plans—AHIP) said he is okay with it, but he reserved the right to change his opinion in the future if necessary. Kristin Abbott (American Council of Life Insurers—ACLI) said she welcomes the change, particularly the removal of Part B. Chris Petersen (Arbor Strategies LLC), representing the Health Coalition, said legislators and state insurance regulators he had spoken with are against including a new private right of action, as the current version in Model #668 would maintain the status quo and not take away any protection from consumers.

Birny Birnbaum (Center for Economic Justice—CEJ) asked for the reason for this change. Johnson said it is because comments received were leaning strongly against the new wording, and no comments had been received leaning strongly in favor of the new wording. Birnbaum asked why the NAIC needs consumer representatives if state insurance regulators are going to do what industry members say. He said privacy differs from security, and the set of company actions differs. He said Model #668 is based on the federal Fair Credit Reporting Act (FCRA), which has a private cause of action, so Model #674 should have it. He posited that if a company takes data without the consumer's consent and the consumer's personal information is stolen, the consumer is harmed. He said a private cause of action would give the consumer an opportunity for redress. He also said this comment is in the comment letter submitted and signed by seven NAIC consumer representatives. Karrol Kitt (University of Texas at Austin) said she supports what Birnbaum is trying to say. She asked how else consumers would get redress. Peter Kochenburger (Southern University School of Law) said he supports what Birnbaum said, and industry never supports any private right of action. Michael DeLong (Consumer Federation of America—CFA) said he agrees with Birnbaum that not having a private right of action would hurt consumers, and it appears state insurance regulators are carrying water for industry. Bonnie Burns (Consultant to Consumer Groups) said she also supports Birnbaum's comments, and it appears that state insurance regulators and industry are on one side of this issue while consumer representatives are on the other side. Birnbaum said there is no evidence or reason for industry to oppose this except for the fact that state insurance regulators can enforce and protect consumers. Harry Ting (Consumer

Healthcare Advocate) said Europe has not been able to control this issue. Birnbaum said there is no status quo on consumers' data. He said we must have a surveillance economy now, and the consequences of losing data are great.

Smock said this change does not affect existing private right of action regulations. He said it depends on the jurisdiction as to whether it has or does not have a private right of action. The new wording allows each state to keep the private right of action or lack thereof that it currently has under law.

2. Discussed the HIPAA Safe Harbor

Johnson said the next topic to be discussed is the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Safe Harbor in Section 19 of Model #674. Petersen said the Health Coalition's comment letter noted that HIPAA preempts state law where it does not conflict and includes a safe harbor that will apply to all HIPAA-compliant companies. He said Model #674 should remove the words "subject to" and only use "compliant with," which is stronger wording. Johnson said Model #674 currently says, "subject to and compliant with." Ridgeway echoed what Petersen said because larger holding companies have health insurers and non-health insurers or companies, so HIPAA should apply to both. He also said the Working Group should want to adopt the most rigid structure regarding data privacy that it can. Birnbaum said the redline in question should say, "... if compliant with HIPAA; not subject to #674," and that it would give safe harbor. He also asked if states would go in to check on whether the companies are HIPAA-compliant. He asked that it be limited to companies that are subject to HIPAA. He also said this is the same as in the *Suitability in Annuity Transactions Model Regulation* (#275), which has caused lots of problems and tremendous confusion holding up even the frequently asked questions (FAQ) document explaining it. Johnson told Birnbaum what he meant by the phrase, "there is no agency to enforce it." Birnbaum said the wording, "subject to HIPAA" would require state and federal oversight of a company that is not subject to HIPAA.

Bradner asked what other lines are only subject to HIPAA, such as health services and property/casualty (P/C) companies compliant with HIPAA. He asked if other lines are subject to HIPAA or Model #674. Birnbaum asked if State Farm says it is compliant with HIPAA, whether states only look at HIPAA or state insurance regulators look at state insurance laws. Petersen said all personal information is protected the same as protected information. He said this is not new. It is in the federal Gramm-Leach-Bliley Act (GLBA) via the *Privacy of Consumer Financial and Health Information Regulation* (#672) and other state legislation via cybersecurity as "compliant with HIPAA." Ridgeway said the concern in California was that companies with HIPAA and non-HIPAA companies both used HIPAA for all lines to create administrative efficiencies, and he is trying to do the same for Model #674. He said an inquiry from the state would resolve any issues, which usually end up checking for clerical error. Aufenthie said it was unclear from the comments submitted by the Blue Cross Blue Shield Association (BCBSA) whether they agreed with the edits being suggested by Ridgeway during this call. Johnson said the comments submitted by the BCBSA referenced personal health information and not the broader term "all personal information," so it was unclear whether the BCBSA was suggesting the same edits as AHIP. She asked Randi Chapman (BCBSA) if she could shed some light on this question. Chapman said she needs to check with her policy person. Johnson asked Chapman to let Lois E. Alexander (NAIC) know if their policy references personal health information or the broader term "all personal information."

3. Discussed Other Matters

Johnson reminded attendees about the in-person interim Working Group meeting to be held in Kansas City, MO, on Monday, June 5, and Tuesday, June 6. She said the purpose of this meeting is to collaborate with state insurance regulators, consumer representatives, and industry members on revised wording for the most complex topics in the new draft of Model #674. Johnson thanked state insurance regulators, consumer representatives, and industry

members who had submitted requests to be added to the registration invitation for this meeting, as the venue limits seating.

Having no further business, the Privacy Protections (H) Working Group adjourned.

SharePoint/NAIC Support Staff Hub/Committees/H Cmte/Privacy/Minutes_PPWG_041823_V2