

Draft: 4/10/23

Privacy Protections (H) Working Group  
Louisville, Kentucky  
March 22, 2023

The Privacy Protections (H) Working Group of the Innovation, Technology, and Cybersecurity (H) Committee met March 22, 2023. The following Working Group members participated: Katie Johnson, Chair (VA); Cynthia Amann, Co-Vice Chair (MO); Chris Aufenthie, Co-Vice Chair (ND); Catherine O'Neil (AZ); LeAnn Crow (KS); Kathleen A. Birrane and Alexander Borkowski (MD); Robert Wake (ME); T.J. Patton (MN); Troy Downing (MT); Martin Swanson (NE); Michael Humphreys and Gary Jones (PA); Patricia Smock (RI); Frank Marnell (SD); Amy Garcia (TX); Mike Kreidler and Todd Dixon (WA); and Rachel Cissne Carabell, Timothy Cornelius, and Lauren Van Buren (WI). Also participating were Peg Brown (CO); John F. King (GA); Doug Ommen (IA); Victoria Hastings (IN); Jo LeDuc (MO); John Arnold (ND); Travis Jordan (SD); and Don Beatty (VA).

1. Adopted its 2022 Fall National Meeting Minutes

Johnson said the Working Group met Dec. 12, 2022. The Working Group also met Mar. 15, 2023, and Feb. 16, 2023, in regulator-to-regulator session, pursuant to paragraph 8 (consideration of strategic planning issues) of the NAIC Policy Statement on Open Meetings, to discuss its next steps.

Amann made a motion, seconded by Aufenthie, to adopt the Working Group's Dec. 12, 2022, minutes (*see NAIC Proceedings – Fall 2022, Innovation, Technology, and Cybersecurity (H) Committee, Attachment Five*). The motion passed unanimously.

2. Heard an Update on Federal and State Privacy Legislation

Jennifer Neuerburg (NAIC) said that there had been a lot of activity since the 2022 Fall National Meeting, but she was going to try to keep her update brief because she knew a lot of people were waiting to comment on the exposure draft. Neuerburg said there are currently around 50 bills under consideration across 21 states.

She said the Iowa legislature passed a consumer data privacy bill on March 15 that is similar to Utah's privacy law and business friendly. While the bill is pending the governor's signature, she said Iowa would become the sixth state to pass a comprehensive data privacy bill. Neuerburg said Hawaii and Indiana are considering bills that are similar to the Virginia Consumer Data Protection Act. She said there are also bills being considered in New Jersey, Montana, and Oklahoma, just to name a few other states.

Neuerburg said charts tracking the legislation will be posted on the Privacy Protections (H) Working Group's web page if anyone wants to read more about these bills. She said the NAIC's legal team will continue to follow state data privacy legislation and provide updates at future Working Group meetings.

Shana Oppenheim (NAIC) said there had been a lot of activity on the federal side. In the House Financial Services Committee, she said Chair Patrick McHenry's (R-NC) financial data privacy bill, the Data Privacy Act of 2023 (H.R. 165) has passed out of committee along party lines. Oppenheim said it would revamp existing data privacy protections for consumers by providing a preemptive ceiling and floor in an attempt to create a uniform federal standard. For enforcement by the functional regulators, the current bill provides a new deletion right for consumers and allows consumers to stop the collection and disclosure of their data, among other provisions. She

said U.S. Rep. Maxine Waters (D-CA) and other Democrats have been critical of the exemption because it would hinder a state's ability to: "Act as a laboratory for innovation while establishing what they see to be a weak federal standard."

Oppenheim said the House Committee on Energy and Commerce has an Innovation, Data, and Commerce Subcommittee that also recently held a hearing like a hearing for a federal national standard on data privacy. She said this follows up on the work from the last Congress, when the House Committee on Energy and Commerce leaders and then senior commerce ranking member, U.S. Sen. Roger Wicker (R-MS), compromised on the American Data Privacy Protection Act (H.R. 8152). Oppenheim said Chairwoman Maria Cantwell (D-WA) did not sign. The bill still passed the House Committee on Energy and Commerce and was being considered for the Omnibus bill, but it was ultimately not included. She said this preemptive bill would create a national standard and safeguards for personal information collected by companies, including protections intended to address potentially discriminatory impacts of algorithms. Oppenheim said the bill is expected to be reintroduced in some form, so federal action is expected to be ongoing.

### 3. Considered its Updated 2023 Work Plan

Johnson gave an overview of the Working Group's updated work plan, dated March 13. She said the workplan is posted on the Working Group's web page and indicates that the exposure draft of the new model was distributed on Feb. 1 for a two-month public comment period ending April 3. Johnson said the revised work plan extends the date by which the model will be sent to the Innovation, Cybersecurity, and Technology (H) Committee to the Fall National Meeting. She said the Working Group did that because it had received so many comments from interested parties, and it wanted to give everyone enough time to consider those comments.

Johnson said the revised work plan lists April 18 as the date that biweekly Working Group meetings will resume to discuss comments received in open meetings. She asked that all parties come prepared to roll up their sleeves and get to work on refining the wording in the draft exposure model.

Johnson said a two-day, in-person, interim Working Group meeting is also being planned for June in Kansas City, MO, to work through the more complex issues identified in the model using transparent collaborations to address those issues in a way that makes the model workable for state insurance regulators, those in the industry, and consumers. She said many of the more complex issues have already been identified by the drafting group in private meetings with volunteer companies. Johnson thanked the companies that had stepped forward to discuss these complex issues. She said many of the industry trade associations and consumer representatives were included in those who volunteered. She said the Working Group was grateful for their help.

### 4. Received and Discussed Comments on the Exposure Draft of the New Model #674

Johnson said the Working Group would hear preliminary comments from interested parties on the exposure draft of the new *Consumer Privacy Protection Model Law (#674)* in advance of the 60-day public comment period ending April 3.

Harry Ting (Healthcare Consumer Advocate) said he was also a Senior Health Insurance Information Program (SHIIP) counselor who has counseled more than 400 people who qualify for Medicare and Medicaid. He said the comments he submitted in more detail in writing on the new draft of Model #674 expressed his strong support for it and suggested a few changes. Dr. Ting said since getting involved in this Working Group, he has become more aware of how personal information is captured and misused. He said whenever he goes to a new website

now, he tries to minimize the data that can be stored and used. He also tries to read the entire privacy policy to understand how to exercise that option. However, he said sometimes it takes too much time, and sometimes, he is given no choice if he wants to use the site. Dr. Ting said he experiences abuse of his personal data daily. He has had his credit card information stolen and gets so many unwanted marketing emails that the emails he wants to see get lost in a sea of unwanted emails. Dr. Ting said the worst of it is that it seems to be occurring more frequently. He said he gets phishing emails and texts disguised as urgent messages from companies he uses trying to steal his personal information. In addition to that, he cannot escape losing his information, as it is being shared by his phone, TV, car, and appliances through the Internet of Things (IoT) in this environment. He said he wishes the federal government would do more to protect his personal information, but that it is unlikely because Google and Meta base their business upon it.

Dr. Ting said now is the time for state insurance regulators to pass fair consumer data privacy legislation for the insurance industry because the key players in this realm are not taking any action. He said he was pleased to see that the draft of Model #674 establishes clear standards for protecting consumer privacy in the areas of: 1) transparency and data minimization; 2) use limitations by review and correction; and 3) requiring third-party service providers to meet the same privacy and accountability standards as licensees. Recognizing that not all states and territories will adopt this model, he said he hopes that many insurance companies and licensees will adopt these privacy protections anyway. By doing so, Dr. Ting said companies are likely to meet the requirements of the states where they do business. He said there are six reasons why consumer data privacy standards are needed and three revisions that he recommends. He said claims that standards are not needed because consumers are not complaining are invalid because consumers have no way of knowing that their data is being used or how it is being shared with others for their use. Dr. Ting said privacy protections must be the default of privacy protection policies should always be the default of non-disclosure. He said it is well documented that most consumers do not read entire privacy policies and that it is not realistic to expect them to do so nor to expect them to understand what is in them because privacy policies are notoriously long and complex. Moreover, Dr. Ting said companies use dark patterns that manipulate consumers into permitting greater use of their data than the consumer had intended.

Dr. Ting said that Health Insurance Portability and Accountability Act of 1996 (HIPAA) standards should apply to all personal information. Dr. Ting said when HIPAA was enacted, it stated that personal health information was more sensitive and needed more protection than personal financial information. However, time has proven that to be false, as personal financial information has been used fraudulently to significantly harm millions of Americans. He said the same standards should apply to third-party service providers as to insurance providers and licensees because the risk of abuse of personal information is the same for both groups. Dr. Ting said because most states do not have regulatory authority over third-party service providers, it is even more important that the model includes these providers in its privacy protection standards through their contracts with insurance carriers that are regulated by state insurance departments. He said data minimization is essential because it is impossible to totally prevent data breaches and that over the past five years, insurance companies as diverse as Prudential Financial, John Hancock, Allstate, and State Farm have each reported multiple data breaches. He said major third-party providers have also reported breaches by Blue Cross Blue Shield Association (BCBSA), a medical imaging group, a professional health care collection agency, and Verisk Analytics—one of the world's largest data aggregators.

Dr. Ting said last month in Congress, the Electronic Privacy Information Center (EPIC) agreed that all companies should limit their data collection to only what is reasonably necessary and appropriate to provide or maintain a product or service requested by an individual. He said that is exactly what is illustrated in the draft of Model #674 and that compliance with it is the key. Dr. Ting said Model #674 will only be effective if it has meaningful penalties

for serious noncompliance because there is no practical way for state insurance regulators to adequately monitor thousands of licensees and third-party service providers. He said there are three specific recommendations:

- Article 3, Section 7, should also require disclosure of consumer reporting agencies used and to the extent they use their third-party services to obtain and share consumers' personal information.
- Article 5, Section 14, should be revised, and it should not be optional because consumers should have the ability to obtain detailed reasons for insurance companies' adverse underwriting decisions immediately and not be required to provide a written request to the company to get those details.
- Data security and privacy are inextricably connected, so data security requirements such as those in the *Insurance Data Security Model Law* (#668) need to be added to this model so third-party service providers and licensees that have access to consumer data are held to the same standards as the insurance companies they contract with.

Johnson said a joint trade group also submitted comments in advance of the comment deadline, which are included in the materials posted on the webpage for this meeting. She asked if anyone would like to provide comments on the draft model.

Kristin Abbott (American Council of Life Insurers—ACLI) said companies and people need standards for privacy protections but do not need an overly prescriptive model. To avoid friction and unnecessary new barriers, she said the key is prior consent for marketing because requiring it would hurt underserved markets, prohibit joint marketing, increase costs and premiums, harm small to mid-sized companies, restrict research, and limit actuarial services. Abbott said overseas processing is difficult to track, and putting privacy restrictions on them would harm international insurers. It would also result in decreased services for customers, which is why the General Data Privacy Regulation (GDPR) does not even require this. She said the 90-day deletion requirement needs to be removed from the model, as most companies with legacy systems will not be able to accommodate this standard. Abbott said the new notice and oversight requirements in the model would increase implementation costs because insurers use personal information to provide products to meet their needs.

Robert Ridgeway (Americas Health Insurance Plans—AHIP) said he was speaking on behalf of both HIPAA-compliant and non-HIPAA-compliant companies. He said the companies he represents like the new timetable and the schedule of future meetings, including the interim, in-person meeting being planned. Ridgeway said the Working Group's plan to handle low-hanging fruit in the form of less complex privacy issues during meetings would be productive. He said the partial exemption for HIPAA issues should be made a complete exemption via safe harbor for HIPAA-compliant companies. Ridgeway said the operative sections should be what companies need to do or not do and should not pertain to activities that are already covered by HIPAA so that companies are not trying to wade through duplicate obligations. He said for other non-HIPAA-compliant companies, the pinch points are: 1) private right of action where verbiage the same as Model #668 would be a good choice; and 2) whether the sharing of personal data overseas should be considered a privacy or cybersecurity issue.

Aufenthie asked that written comments be submitted describing where in the model the partial safe harbor for HIPAA (Sections 2, 9, 10, 11, 12, or 13) should be changed to a full safe harbor incorporating oversight of third-party contracts, including business associates and how they think it should be worded.

Shelby Schoensee (American Property Casualty Insurance Association—APCIA) said that several members have met with the drafting group. They want an in-person interim meeting, will be submitting written comments, and will be actively engaged in the collaboration process. She said their primary concerns are: 1) the overseas data privacy requirement because many of the companies operate on a global basis that relies on the data market; 2)

the marketing and research limitations, as they would prevent joint marketing; 3) third party oversight, which is a contractual issue, so a delayed effective date (like the risk-based approach in Model #668) for implementation is imperative; 4) the private right of action; 5) the new notice requirements; and 6) the inconsistent language about actuarial studies. Schoensee said the Working Group needs to find an appropriate balance between a consumer's needs and a company's right to market its products.

Birny Birnbaum (Center for Economic Justice—CEJ) asked what an appropriate balance between consumer needs and company marketing would be.

Commissioner Humphreys said this question came up with the ACLI, AHIP, and now the CEJ. Ridgeway took a little different tact with the unsolicited sales and marketing by saying state insurance regulators do not want to curtail a company's ability to do that, whereas Schoensee and Ridgeway both mentioned wanting to protect policyholders' money and not wasting it. He said he was trying to figure out what the balance was because he would argue that a lot of the unsolicited sales that he gets today are a waste. Commissioner Humphreys said there is a bit of a challenge here. He equated this to a non-insurance example of closing on a house and then getting 73 calls about the mortgage rate for the next two days—all unsolicited and all unwanted—blocking his phone. So, then, where do we draw the line if we are concerned about the policyholders' money but also want you to be able to continue to make these offers? Schoensee said that finding the balance is one of the issues that need to be addressed in the in-person meeting.

Wes Bissett (Independent Insurance Agents and Brokers Association—IIABA) said he was surprised by the draft because the changes to it were so extensive and that the Working Group had gone too far in restricting companies' and producers' use of consumer data. He said it should be much broader to allow licensees to operate efficiently.

Aufenthie suggested that the IIABA submit detailed written comments with specific reasons why existing wording would not be effective and suggest new wording that would address the pain points noted rather than giving broad disapproval of the draft model out of pocket without providing constructive criticism or solutions.

Chris Peterson (Coalition of Health Insurers) said HIPAA preemption changes to the proposed privacy rule should be reworded to read, "if companies comply with" rather than "is subject to," and that it should be a safe harbor for those companies deemed to be HIPAA-compliant rather than an exemption. He said other sections brought under the safe harbor would be business associate agreements for third-party businesses because health care providers expect to see it in order to keep a lack of confusion, as he said HIPAA is more robust than the draft model in all areas. Aufenthie suggested that health care providers go through each of the sections in the model, indicating where in HIPAA the sections could be found that indicated more robust consumer data privacy than that in the draft model. Peterson said the offshore data issue is a federal constitutional issue and that there should be no private right of action due to federal labor issues.

Cate Paulino (National Association of Mutual Insurance Companies—NAMIC) said that the opt-in requirement was a showstopper, especially when it came to sharing data outside of the U.S., as companies would lose their efficiencies by providing servicing for consumers 24/7. She said the annual notice requirement violated the federal Fixing America's Surface Transportation (FAST) Act, which eliminated the need to send annual notices and has been enacted in 47 states. Paulino said the model should use categories of sources for data minimization, not be so prescriptive, and not limit the application process because hundreds of thousands of licensees would be subject to contract issues. She said that exemptions were necessary as are delayed effective dates to comply. Paulino said that exclusivity as to insurance versus general business practices should be implemented and that there should be no private right of action.

Jeffrey Klein (McIntyre & Lemon) asked that the Working Group reconsider the wording of Article 4, Section 4, and said that he would submit detailed suggestions as to the changes along with his clients' reasons for requesting such changes. Wake said the deletion of marketing was intentional due to the cause versus benefit analysis. Peter Kochenburger (Southern University of Law—SULC) said it was this issue that caused Wells Fargo to be forced to sell its insurance business and financial products in order to prevent massive fraud. Johnson said this issue would be one of the more complex issues that would be addressed at the in-person interim meeting.

#### 5. Discussed Other Matters

Johnson reminded attendees about the Working Group's two-day, in-person interim meeting tentatively scheduled for June 4–6 in Kansas City, MO.

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

SharePoint/NAIC Support Staff Hub/Committees/H Committee/2023\_Spring/Minutes\_National Meeting\_PPWG\_Final