Draft date: 11/21/23

2023 Fall National Meeting
Orlando, Florida

PRIVACY PROTECTIONS (H) WORKING GROUP
Friday, December 1, 2023
11:30 a.m. – 12:45 p.m.
Bonnet Creek Hilton - Floridian Ballroom D-F & Corridor II - Level 1

ROLL CALL

Katie Johnson, Chair	Virginia	Jeff Hayden	Michigan
Cynthia Amann, Chair	Missouri	T.J. Patton	Minnesota
Chelsy Maller	Alaska	Molly Plummer	Montana
Gio Espinosa/Catherine O'Neil	Arizona	Martin Swanson	Nebraska
Damon Diederich/ Jennifer Bender	California	Santana Edison	North Dakota
		Teresa Green	Oklahoma
George Bradner/Kristin Fabian	Connecticut	Raven Collins	Oregon
C.J. Metcalf/ Erica Weyhenmeyer	Illinois	Richard Hendrickson/ Gary Jones	Pennsylvania
Victoria Hastings	Indiana	Patrick Smock	Rhode Island
LeAnn Crow	Kansas		
Ron Kreiter	Kentucky	Frank Marnell	South Dakota
Robert Wake/Sandra Darby	Maine	Todd Dixon	Washington
Van Dorsey	Maryland	Lauren Van Buren/ Timothy Cornelius	Wisconsin

NAIC Support Staff: Lois E. Alexander/Jennifer Neuerburg

AGENDA

1. Consider Adoption of its Summer National Meeting Minutes—*Katie Johnson (VA)* — Attachment 1

2. Hear an Update on State Privacy Legislation and Federal Privacy Activities—*Jennifer Neuerburg and Shana Oppenheim* — Attachment 2a and 2b

3. Discuss Next Steps in the Working Group's Process for Moving Forward with Drafting the New *Insurance Consumer Privacy Protection Model Law* (#674)—*Katie Johnson (VA)* — Attachment 3

4. Discuss a Referral from the Risk Retention Group (E) Task Force —*Katie Johnson (VA)* — Attachment 4

5. Hear a Presentation on Access to Data, Costs, and Inherent Privacy Risks in Legacy Systems vs. Non-Legacy Systems—*Eric Ellsworth, Data Scientist (Consumers' Checkbook/ Center for the Study of Services) – 45 minutes*

6. Discuss Any Other Matters Brought Before the Working Group —*Katie Johnson (VA)*

7. Adjournment

Draft Pending Adoption

Attachment --
Innovation, Cybersecurity, and Technology (H) Committee
8/13/23

Draft: 8/30/23

Privacy Protections (H) Working Group
Seattle, Washington
August 13, 2023

The Privacy Protections (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met in Seattle, WA, Aug. 13, 2023. The following Working Group members participated: Katie Johnson, Chair (VA); Cynthia Amann, Vice Chair (MO); Lori K. Wing-Heier (AK); Catherine O'Neil (AZ); Damon Diederich (CA); George Bradner (CT); Erica Weyhenmeyer (IL); LeAnn Crow (KS); Ron Kreiter (KY); Van Dorsey (MD); Robert Wake and Sandra Darby (ME); Jeff Hayden (MI); T.J. Patton (MN); Santana Edison represented by Colton Schulz (ND); Martin Swanson (NE); Teresa Green (OK); Raven Collins (OR); Gary Jones (PA); Patrick Smock (RI); Frank Marnell (SD); Todd Dixon (WA); Rachel Cissne Carabell and Timothy Cornelius (WI). Also participating were: Sarah Bailey and Heather Carpenter (AK); Peg Brown (CO); Doug Ommen (IA); Victoria Hastings (IN); Jamie Sexton (MD); Eric Dunning (NE); Judith L. French (OH); Matthew Tarpley (TX); and Don Beatty (VA).

1. Heard Opening Remarks

Johnson said the Working Group has what looks like a simple agenda, but it has important discussions ahead of it. She said she and the Working Group would like to thank everyone who has been and continues to be an important part of this transparent, collegial, and collaborative process, especially those who spent considerable time, money, and input for two full days—four days including travel time—to dig into seven important issues with the model.

Johnson said she would like to give an update on the Working Group's activities to ensure all stakeholders are on the same page going forward. She said the 60-day comment period for the first draft of the new *Insurance Consumer Privacy Protections Model Law* (#674) ended April 3.

Johnson said the drafting group met with companies privately to discuss current consumer data practices on May 9, May 4, April 28, April 27, April 20, April 13, April 12, April 11, April 6, and April 5.

Johnson said the Working Group met July 25, June 5–6 at an in-person meeting in Kansas City, MO; May 16; May 2; April 18; and at the Spring National Meeting to discuss comments received and collaborate on workable language. She said the interim meeting sessions were working sessions focused on the drafting of model language. She said the 112 in-person attendees—29 state insurance regulators, including one commissioner; three NAIC consumer representatives; 68 industry representatives; and 12 NAIC staff members—were asked to be prepared to consider new language and offer their pros and cons. She said participants were asked to keep their comments specific to the topic under discussion. She said topics already discussed in open meetings were not revisited during this meeting.

Johnson said a drafting group met Aug. 9, July 20, July 10, July 7, June 30, June 29, June 26, June 23, June 2, May 17, May 12, and May 5 in regulator-to-regulator session.

Johnson said because Version 1.2 of the new Model #674 was based on changes discussed at the interim meeting, the Working Group exposed it July 11 for a public comment period ending July 28. She said the drafting group privately continued its meetings with industry trades and companies to discuss current consumer data practices Aug. 9, meetings with two different companies on Aug. 3, Aug. 2, and July 28.

Draft Pending Adoption

Johnson said the Working Group sent interested parties an invitation that it would continue scheduling private calls with trades, companies, and other interested parties. She said the Working Group also notified interested parties that so many comment letters had been received since the interim meeting that the Working Group has been unable to post them all prior to the Summer National Meeting. She said the Working Group will continue posting comments to the website after the national meeting. She said due to the sheer volume of comments and the number of one-on-one calls requested, the Working Group has determined that more time is needed to engage the public and continue drafting the model.

2. Adopted its July 25, June 5–6, May 16, May 2, April 18, and Spring National Meeting Minutes

Johnson said the Working Group met July 25, June 5–6, May 16, May 2, and April 18. During its meetings, the Working Group took the following action:

A. Discussed comments received and collaborated on workable language regarding the following seven topics:
   i. Third-party service providers, including the definition of third-party service providers, third-party service providers not related to an insurance transaction but that have access to consumers' personal information, and contracts with third-party service providers.
   ii. Definitions of insurance transactions and additional permitted transactions.
   iii. Marketing, including marketing insurance products to consumers using consumers' personal information, marketing other products to consumers using consumers' personal information, and affiliate marketing.
   iv. Joint marketing agreements (JMAs), JMAs with affiliates, and JMAs with non-affiliated third parties.
   v. Opt-in versus opt-out consent to marketing and the difference between marketing insurance and non-insurance products.
   vi. Notice of Consumer Privacy Practices – Contents.
   vii. Notice of Consumer Privacy Protections – Frequency and Methodology of Delivery.
B. Drafted Model #674 language. In-person attendees were asked to be prepared to consider the new language and offer pros and cons. Participants were asked to keep their comments specific to the topic under discussion. Topics already discussed in open meetings were not revisited during this meeting.
C. Exposed Version 1.2 of the new Model #674 on July 11 because it was based on changes discussed at an interim meeting, with a public comment period ending July 28. The drafting group continued its meetings with industry trade companies privately Aug. 9, Aug. 3, Aug. 2, and July 28 to discuss current consumer data practices.
D. Notified interested parties that so many comment letters have been received since the interim meeting that the Working Group has been unable to post them all prior to the Summer National Meeting. The Working Group will continue posting comments to the website after the national meeting. Due to the sheer volume of comments and the number of one-on-one calls requested, the Working Group has determined that more time is needed to engage the public and continue drafting Model #674.
E. Discussed comments received and engaged the public to continue drafting Model #674.

The Working Group also met Aug. 12 in regulator-to-regulator session, pursuant to paragraph 4 (internal or administrative matters of the NAIC or any NAIC member) of the NAIC Policy Statement on Open Meetings.

Amann made a motion, seconded by Diederich, to adopt the Working Group's July 26 (Attachment A5), June 5–6 (Attachment A4), May 16 (Attachment A3), May 2 (Attachment A2), April 18 (Attachment A1), and March 22 (*see*

NAIC Proceedings – Spring 2023, Innovation, Cybersecurity, and Technology (H) Committee, Attachment Three) minutes. The motion passed unanimously.

3. Heard Updates from NAIC Staff on State and Federal Privacy Legislation

Jennifer Neuerburg (NAIC) said in the continuing absence of congressional action on a comprehensive U.S. federal privacy law, many states have enacted state data privacy laws or are considering legislative action. She said on June 30, the Delaware legislature passed the Delaware Personal Data Privacy Act (HB 154), and the bill is ready for governor consideration. She said assuming that the bill becomes law, Delaware will become the 12th state—the seventh this year—to pass a consumer data privacy law. The other states that have passed bills this year are Indiana, Iowa, Montana, Oregon, Tennessee, and Texas. Neuerburg said at least 16 additional states have introduced data privacy bills during the current legislative cycle that are either comprehensive in nature or address a range of data privacy issues, and if anyone wants to read more about these bills, there are charts tracking state legislation on the Working Group's web page.

Shana Oppenheim (NAIC) said the privacy legal and regulatory landscape is changing quickly in the U.S., particularly for financial institutions, which hold significant volumes of consumer data. She said at the federal level last year, the U.S. Congress (Congress) made significant bipartisan progress on comprehensive federal privacy legislation, advancing the proposed federal American Data Privacy and Protection Act (ADPPA), which passed out of the U.S. House of Representatives (House) Committee on Energy and Commerce with a 53-2 vote and almost made it to a House floor vote. Earlier this year, she said the House Committee on Energy and Commerce's new Subcommittee on Innovation, Data, and Commerce held a hearing in March titled "Promoting United States Innovation and Individual Liberty Through a National Standard for Data Privacy." Additionally, she said House Financial Services Committee Chair, Patrick McHenry's, financial data privacy bill, the Data Privacy Act of 2023 (H.R. 1165), passed out of the Committee along party lines in February. She said it would: 1) revamp existing financial privacy protections for consumers under the federal Gramm-Leach-Bliley Act (GLBA); and 2) create a preemptive ceiling and floor to create a uniform federal standard. She said the current bill allows for enforcement by functional regulators, provides a new deletion right for consumers, and allows consumers to stop collecting and disclosing their data, among other provisions. She said Representative Maxine Waters (D-CA) and the Democrats have been critical of any preemption because it would hinder the states' ability to act as a laboratory for innovation while establishing a weak federal standard. She said although there seemed to be some legislative momentum earlier this year, nothing has yet come of it. She said more limited/focused data privacy actions seem more likely. For example: 1) the House Judiciary Committee also approved a bill in July that would ban law enforcement agencies from buying people's sensitive information from data brokers—the Fourth Amendment Is Not For Sale Act; and 2) for the second consecutive year, the U.S. Senate (Senate) has approved two children's online privacy measures—the Kids Online Safety Act (KOSA)—for floor consideration just before departing for the month-long August recess. Oppenheim said KOSA is focused on social media companies and children's data. She said U.S. state insurance regulators are also drafting several regulations that may be pertinent: 1) the Consumer Financial Protection Bureau (CFPB) is in the process of issuing a rule for the long-awaited implementation of Section 1033 of the federal Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), which would require that consumers be able to access their financial data. She said the rule may specifically affect checking, savings, and credit card accounts. It is expected later this year with a final rule slated for 2024; 2) the CFPB also launched an inquiry into data brokers under the federal Fair Credit Reporting Act (FCRA), and it is attempting to understand the "full scope and breadth of data brokers and their business practices, their impact on the daily lives of consumers, and whether they are all playing by the same rules." She said the Federal Trade Commission (FTC) is also investigating commercial surveillance industries, which it defines as collecting, analyzing, and profiting from information about people. She said the term encompasses the collection, aggregation, analysis,

retention, transfer, or monetization of consumer data. She also said in an advanced notice of proposed rulemaking in August 2022, the FTC posed 95 questions about consumer harm, data security, and related topics to commercial surveillance companies.

4. Discussed an Extension to Develop the New Model #674

Johnson said the Working Group would like to discuss an extension of the time to develop the new Model #674 due to the sheer volume of comments received on Version 1.2 from July 11 through Aug. 8 and the number of requests for private calls with trade associations, consumer representatives, and companies.

Johnson said the 15 comment letters received prior to the July 28 due date are posted to the Working Group's web page and the meeting platform in the Summer National Meeting Event App. She also said the eight comment letters received after the July 28 due date will be posted to the Working Group's web page following the Summer National Meeting. She said the Working Group received 32 separate comments and redlined language documents in total. Additionally, she said the Working Group needs to review previously received comments to ensure all comments have been considered.

Johnson said extending the timeline would give the Working Group the time it needs to review all the comments submitted and have conversations with those who submitted the comments to ensure all stakeholders are heard and all parties understand the functional differences between different licensees and the various types of insurance being offered to consumers.

Johnson said the next version of the draft would be a redline that includes comments submitted, and the exposure draft period would allow a reasonable time of four to six weeks to review and comment on it. She said the Working Group will probably have another interim meeting before the Fall National Meeting, when a new timeline will be presented. Crow read a statement indicating that more work and time is needed for the state to support the draft model. Hastings thanked the Working Group for all its efforts in drafting a model that could work for all stakeholders, and she said Indiana has concerns that the interested state insurance regulators will work with the Working Group to resolve.

5. Discussed the Sections on Marketing, Consumer Notices, and Opt-Out/Opt-In in the Second Exposure Draft of Model #674

Johnson said the next item on the agenda is to discuss the topics on which the most comments were received; i.e., marketing, consumer notices, and opt-in/opt-out. She said the Working Group would hear from anyone who would like to talk about these topics. She asked that each stakeholder limit their comments to three minutes if possible and please focus on what, in their opinion, works and what does not. She said this will give Working Group members and other state insurance regulators time to ask questions and discuss the issues presented. Marnell reiterated the comments he submitted on the first exposure draft of the model prior to the Working Group's interim meeting in June, indicating that South Dakota could not support Version 1.2 of the model in its current form. Swanson said Nebraska agreed with the comments submitted by Marnell.

Shelby Schoensee (American Property Casualty Insurance Association—APCIA) said she appreciates all the hard work the Working Group put into Version 1.2 of the model, but she is disappointed that it did not include all of the APCIA's comments from the interim meeting in June. She said it was a patchwork of extensive regulatory changes that included unworkable notice requirements, such as obtaining consumers' signed consent for insurance data retention, sharing, and annually renewable data review, so it needs more work.

Kristin Abbott (American Council of Life Insurers—ACLI) said the drafting group was clearly dedicated given the tremendous amount of work that had already been accomplished, and she said she appreciated working with the drafting group on specific issues of concern to her members. She said, however, that a redline document would allow the most constructive feedback to be given to avoid conflicting verbiage. She also said she was extremely disappointed that the ACLI's ideas about JMAs, marketing, retention, deletion, and data correction had not been included.

Karrol Kitt (University of Texas at Austin) said state insurance regulators need to know that consumers need this revised model desperately, and consumers need their help in protecting personally identifiable information because most insurance consumers do not understand the implications of what happens to their data once companies share it with other non-insurance companies.

Lauren Pachman (National Association of Professional Insurance Agents—PIA) said she submitted comments on behalf of the PIA's members last week and was surprised that the adverse underwriting decision language had been kept in Version 1.2 of the model. At the interim meeting in June, she said she asked that the National Flood Insurance Program (NFIP) be fit into the draft model because only 10% of consumers buy flood insurance directly through the NFIP. Agents are selling it to the other 90% of consumers through an arrangement with the federal government—via federal government borrowing money or the Federal Emergency Management Agency (FEMA) through upstream and downstream agreements—that could be considered a JMA in this model. Pachman said most flood policies sold cover $250,000, and agents sell flood insurance for homes over that amount to ensure full coverage for homeowners. She asked how agents could offer this excess coverage under the model and if agents would need to get the consumer's approval in advance via written consent, which would be a potential errors and omissions (E&O) problem for consumers.

Johnson said she would be happy to set up a call with Pachman to discuss the sale of flood insurance further, as this concern was an unintentional consequence. She said she still believes state insurance regulation is better for consumers than federal regulation. Diederich said he believes the model has the same definition of financial institution as the federal government. Johnson confirmed that it is in Version 1.2.

Harry Ting (Health Consumer Advocate) said the new state insurance regulatory protections are sorely needed. He said the model is not confusing to consumers. For Sections 9 and 10 of Model #674, he suggested creating a standard template for consumer notices that could be clearly understood and uniform; i.e., like those created for the Medicare program.

Matthew J. Smith (Coalition Against Insurance Fraud—CAIF) said he submitted written comments on July 27 and urged state insurance regulators to update the model to protect consumers against insurance fraud. He asked the Working Group to focus on two issues: 1) consider making sure investigations of insurance fraud can continue by taking care not to prevent such investigations inadvertently; and 2) take the opportunity to designate fraud prevention clearly.

Peter Kochenburger (Southern University Law School) said he supports the revision of the model and understands that whether consumers should be given the opportunity to opt-in or opt-out of sharing their personal information is always the question. He said opt-in should be the default because opt-out means companies will share a consumer's personally identifiable information with their affiliates. Industry understands this, so that is what they prefer. Kochenburger said it is up to the Working Group to determine if consumers can have the protection of an opt-in consent that would provide the opportunity for consumers to know what they are agreeing to. He said he recently signed up for the highest level of Wi-Fi access, and the acceptance of the terms included several pages of

legalism in very small print that was hard to read, even for an attorney. He said the only realistic opportunity for consumers to control the use of their data is an opt-in consent form. Kochenburger said the creation of an opt-in consent form is a complicated topic that needs further consideration. He said the Working Group has done a great job of putting together real consumer protection provided through state insurance regulation, whereas the federal government could adopt a broad bill.

Diederich said due to the GLBA, JMAs make it difficult to do this, and he needs ideas from Kochenburger on banks.

Wes Bissett (Independent Insurance Agents & Brokers of America—IIABA) said his members have threshold concerns, and he agrees that privacy is important, as is uniformity. He said the disagreement is on how to do it. He said the GLBA is wonderful, and the Working Group needs to use it. He said he has carried a lot of water for state insurance regulation over federal insurance oversight throughout the years because he supports state insurance regulation. However, he said he believes the Working Group should discontinue drafting a new model to replace the *NAIC Insurance Information and Privacy Protection Model Act* (#670) and the *Privacy of Consumer Financial and Health Information Regulation* (#672). He also said Model #670 and Model #672 only need minor adjustments, as they have worked well for many years.

Amann said she was actively involved when Model #672 was drafted in 1992, and the new model is being conscientiously drafted with language referred from Model #670 and Model #672. She said it would be helpful if Bissett could tell the Working Group where exactly it went off the rails because lines of business are different, as are companies' business processes. She also said new technologies have been and are being brought to the table, which is why the Working Group would appreciate any direction regarding Bissett's members' concerns.

Cate Paolino (National Association of Mutual Insurance Companies—NAMIC) said she appreciates the drafting group's willingness to discuss issues of concern in the model with her members. She highlighted the importance of making the new model more workable for companies, and she asked that it be more like California's privacy regulations. She pointed out that the timeline in Section 5 of Version 1.2 is three times longer than it is in California; instead, it should be in alignment with California, like railroad tracks, rather than trying to change the entire landscape of privacy, which would take a major effort on the part of insurance companies. She asked if there was any need to go beyond what California or Model #672 did, particularly Sections A.6 and A.7 of the new model. She said these sections address marketing across jurisdictions, which should not be a topic for a privacy discussion. She said her members continue to be willing to work with the Working Group to revise the wording in Version 1.2 to address these outstanding issues.

Erica Eversman (Automotive Education & Policy Institute—AEPI) said she echoes the thoughts of the other consumer representatives, and she suggested specifically identifying certain types of data categories by looking to California, as companies are already complying with it. She said other personally identifiable information, such as commercial, financial, banking, internet, browsing, fingerprints, voice prints, geo data, audio, visual, education, and professional/employer information, should be considered as inferences that industry could use to create a profile that could lead to automotive insurance disputes. She said bodily injury under personal injury protection (PIP) auto insurance requires that the consumer waives federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) rights to give access to health information for claims. She asked if this gives other companies access to medical data that they would not normally have due to HIPAA protections.

Eric Ellsworth (Consumers' Checkbook) said he is a data scientist with both an information technology (IT) and a HIPAA background who believes in strong data protection. He said there has been a lot of discussion about the inability of companies to access data in legacy systems to correct or delete a specific consumer's data when it is

no longer needed. He said while it is true that legacy systems require a lot of maintenance and a lot of work, it is not true that data in legacy systems is safe because companies cannot access it. He said an experienced data scientist can access data located anywhere and from any type of system, including a legacy system. He said it is also true that companies may not know what data they have or where the data they have accumulated, especially through agreements, mergers, and acquisitions of blocks of business from other companies, is located. He said contrary to what is being said about consumers having to pay higher premiums to cover the additional costs companies will incur to comply with the new privacy act, history has proven that not to be the case. He said the same thing was said about HIPAA and California's privacy law, yet neither HIPAA nor California privacy compliance has bankrupted any insurers. He said state insurance regulators need to bind companies to the same rules as HIPAA, and he encouraged state insurance regulators to maintain this level of control over consumers' data.

Diederich said the Parliament of India recently enacted very strong data privacy protections with a data fiduciary requiring consent. He said this is a level setting, as the U.S. is very technologically advanced but not very advanced in privacy protection.

6. Discussed Other Matters

Johnson reminded attendees about the Insurance Summit, Sept. 11–14.

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

SharePoint/NAIC Support Staff Hub/Committees/H Committee/2023 Summer/WG-Privacy/Minutes_Summer 23 NM_PPWG

Privacy Protections Working Group

Process for Moving Model #674 Forward
October 25, 2023

To address the feedback received related to the privacy model development and to continue with this important work, the Working Group's Chair has worked with NAIC staff to develop the following plan.

The goal of this process is to move the privacy model forward towards a third draft to be exposed for public comment and to promote the Working Group's future process in the interest of increasing transparency and stakeholder collaboration while ensuring the work proceeds in an orderly manner with regular involvement from the H Committee leadership.

Based on this process, it is anticipated that the next draft of the model will be available after the first of the year in 2024. An integral part of this process is the Working Group's request for an extension of one year to allow the Working Group to move at a pace that is sustainable.

Process

- The Working Group Chair and volunteer regulators have created a Comment Chart that will be used by the Working Group throughout the process. This chart will allow the Working Group to ensure the inclusion of all comments received from states, industry, and consumers broken down by model section.
    - This chart will be beneficial in helping regulators understand the feedback that has been received and how the next version of the model addresses the input.
    - Working Group responses and revised language will be captured in the Comment Chart as well**.**
- The Working Group will hold a regulator-only call to discuss the process moving forward that will include an explanation of how the Comment Chart will be utilized.
- The Working Group will have regulator-only calls when necessary. These will be regulator only sessions because the discussion or action contemplated will include 3. Specific companies, entities, or individuals, and 8. Consideration of strategic planning issues relating to regulatory matters.
- Regulator-only Working Group one-on-one meetings with entities will be held when requested by entities.
- The Working Group Chair will provide Monthly Reports to the H Committee Chair.
- The third draft of the new model will be exposed to regulators for a regulator comment period prior to its exposure to the public for a 60-day comment period early in 2024.
- The new draft will contain revision marks to reflect all changes made to the draft dated July 11, 2023.
- The Working Group anticipates sending the final model to the H Committee to consider for adoption at the 2024 Fall National Meeting.

Reasons for Request for Extension

- An extension will allow for multiple engagement points and comment periods.

- An extension will allow regulators and interested parties to review draft 2.0 thoroughly and develop meaningful comments to share with the Working Group.
- An extension will give the Working Group time to carefully consider input from all stakeholders and to create the best work product.

NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

MEMORANDUM

TO: Members of the Privacy Protection (H) Working Group

FROM: Risk Retention Group (E) Task Force

DATE: October 13, 2023

RE: Applicability of *Insurance Consumer Privacy Protection Model Law* (#674) to RRGs

---

The Risk Retention Group (E) Task Force recently met and discussed the applicability of the *Insurance Consumer Privacy Protection Model Law* (#674) to risk retention groups (RRGs). Based on the review of the draft, it appears that it applies to the domiciliary states of RRGs given that "Insurer" as defined only excludes foreign risk retention groups. The Task Force noted that draft Model #674 will replace the *Privacy of Consumer Financial and Health Information Regulation* (#672). Further, the Task Force commented that Model #672 does not apply to information about companies or about individuals that obtain products or services for business or commercial purposes. Therefore, it was not applicable to RRGs, while it appears that draft Model #674 does not have a similar express limitation to personal lines insurance.

Since the requirements of draft Model #674 focus on individual consumers, it is unclear whether it is intended to protect the personal information of individuals that may be collected in connection with a commercial lines insurance transaction. If this is the case, draft Model #674 would be applicable to domestic RRGs. The Task Force greatly appreciates any clarification you provide with regard to draft Model #674. Should you have any questions, feel free to contact Andy Daleo (adaleo@naic.org) or Rodney Good (rgood@naic.org).

Legacy Systems and Protection of Consumers' Privacy

Eric Ellsworth, MS MBA

Director Health Data Strategy

CONSUMERS' CHECKBOOK

Overview

- Consumers views on privacy
- Impacts of Privacy Breaches
- What are legacy systems why do they pose problems?
- Processes to bring control to systems and data
- Considerations for regulation

Organizational and Personal Background

Consumers' Checkbook/ Center for the Study of Services

- Nonprofit helping consumers choose services including many lines of insurance
- We develop independent, unbiased evaluations and data and publish to consumers
  - Checkbook Magazine (checkbook.org)
  - Survey research on healthcare quality (CAHPS, HEDIS, etc.)
  - Plan shopping websites for SBMs, DOIs, others
- Advocates for transparency and simplification of consumer experience

Eric Ellsworth

- Technologist and Data Scientist
- NAIC Consumer Representative
- Started my career doing technology for a cardiac surgery practice/hospital research group
- 10 years at a clinical lab providing novel genomic testing for cancer risk
  - Built data systems
  - Ran innovation, clinical trials
  - HIPAA Privacy and Security officer
- Currently work simplifying insurance plan selection and other healthcare shopping

Consumers Are Increasing Concerned About Privacy

- More than 75% of consumers are concerned about the privacy of their data
- Nearly half of consumers would walk away from a financial services company if they could not restore service in 3 days (Arcserve 2020)
- Consumers value companies that protect their privacy and will leave ones that don't

CONSUMERS' CHECKBOOK

Consumers Cannot Protect Their Own Data

They have:

- No authority or accountability over systems holding their data
- No idea who is putting their data at risk
- No professional expertise in cybersecurity
- A reasonable expectation that an insurer takes the right steps to protect data gained through ordinary business transactions

So regulators must:

- Ensure that there are mechanism for viewing, fixing, and deleting data
- Provide accountability for breaches and misuse of our data
- Protect them from problems with their insurance arising from

CONSUMERS' CHECKBOOK

Impact of Data Breaches on Insurers

- Financial losses or bankruptcy
  - Average ransomware attack costs = $4.65 M
  - US insurers have paid up to $40M
  - Often millions or tens of millions of dollars in lawsuits
  - Remediation Time and Costs
- Damage to company's brand
- Operational paralysis
  - Ransomware – typically 22 days to normal operations
  - Much longer in retroactive work fixing systems

- Insurers are a high value target due to holding lots of data and money
- >50% of largest insurance carriers are 3x more likely to experience breaches
- Software vendors are the most common source of digital supply chain attacks

Impact of Data Breaches on Consumers

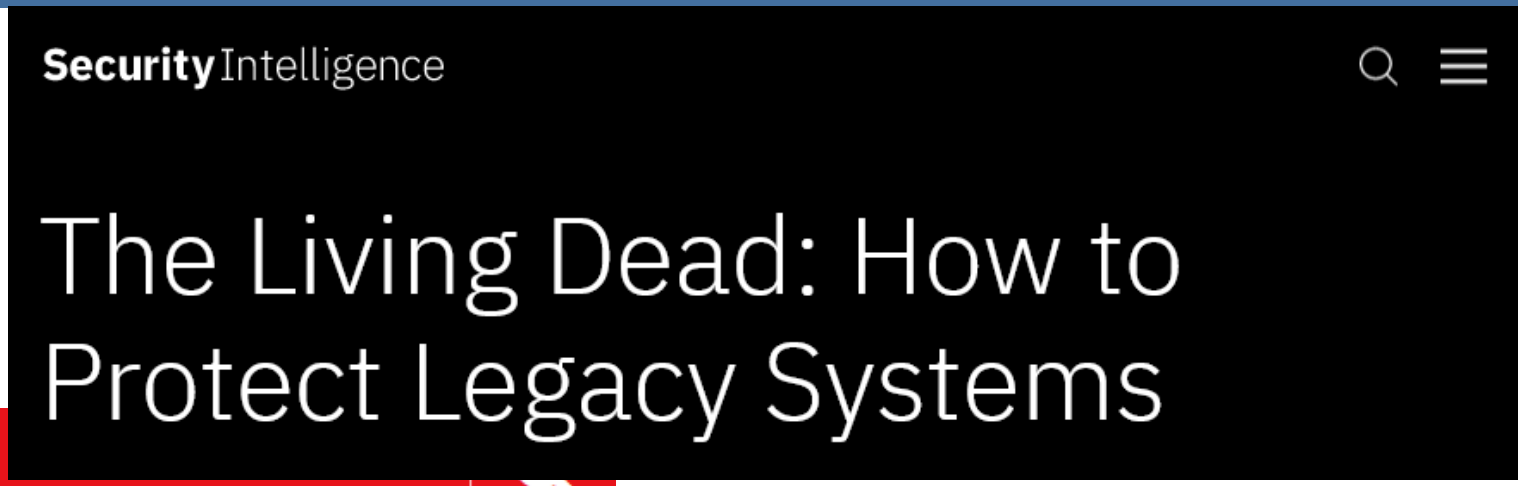
Direct Effects

- Identity theft - >45M people, $56B in losses
- Data taken in one breach can be used in other attacks

Insurance Problems

- Insurer Cannot Pay Claims (ransomware, insolvency)
- Unexpected premium increases post-attack
- Unavailability: Insolvency or withdrawals can damage entire markets

Legacy Systems



What Exactly Are Legacy Systems?

- Legacy systems are software that is outdated but still in operation
  - No longer actively maintained, upgraded, or supported
  - No personnel with active knowledge of how system works and what's in it
  - Some are still used for core business functions

- Many legacy systems are in the shadows
  - People don't know that they're there, what they do, and what if anything about them is still needed and used
  - Path of least resistance is to leave them alone

What Is Legacy Data?

- Legacy data is data that an organization still possesses that may or may not be in use
- Often in obsolete or proprietary data formats
  - Data can only be accessed by retaining the legacy system that wrote it
  - Alternative is to migrate all data to new formats
- Immediate business need often does not justify the effort of migrating all data
- Data gradually fades from view… but is still there in the shadows
  - Old servers, hard drives from laptops, email accounts, third party email accounts
  - In closets, basements, storage units, garages, empty offices

Legacy Systems are Highly Vulnerable

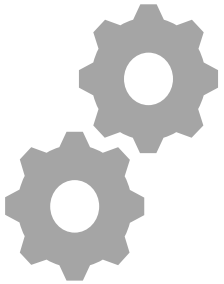
- Older systems often developed with less attention to security
  - Written in old programming languages that did not prioritize security
  - Use libraries with known security issues
- May require old hardware, operating systems (e.g. Windows NT), or databases
- Many were designed assuming a private network, not modern internet-connected networks that can be accessed from around the world
- Vulnerabilities are not patched because the system is end-of-life

- A garden of delights for hackers

Why Are Legacy Systems Hard to Get Rid Of?

Typical migration:

- Get new system running, keep old system running
- Migrate only the data needed to get the new system running
- Find problems or missing data and go back to old system
- Old system stays running “just in case”
- Attention moves on to new system, leaving old system and data as it was
- Nobody knows what the old system is doing or where the data is



Proactive decommissioning:

- Thoroughly inventory of old systems, plus their data and functions
- Assess needs for all data, risks of destroying vs keeping
- Migrate all data to new systems
- Dispose of old systems & data (e.g. take down servers, properly destroy hard drives)
- Maintain inventory and security control of old data

Controlling Risks of Legacy Systems and Data

- Inventory of System and Data Assets
- Evaluate needs, risks, costs of keeping vs replacing each asset
- Prioritize Actions
  - Correctly Decommission Unneeded Systems and Data
  - Consolidate and secure needed legacy data
  - Transition to new systems where feasible
  - Add security measures around legacy systems that are still needed

- Having control of data depends on management and oversight processes, regardless of which systems hold the data

Effective Oversight is the Key to Delivering Privacy

To minimize data held on consumers, meet amendment/deletion requirements, and effectively manage cybersecurity risks requires inventory and ongoing control of data across all systems

Well prepared organization

- Knows where nearly all the records for any customer are
- Has immediate access to those records
- Consolidated old records into central storage systems
- Identified and removed or locked down unnecessary legacy data and systems
- De-identified or aggregated data to retain knowledge of customer behavior

Unprepared Organization

- Only knows about customer records in a few primary systems
- Does not know what other customer data it holds
- Needs ad-hoc work to figure out where data on a customer is
- Doesn’t know all the systems it is running
- Lacks immediate access to older systems and data

Legacy Systems Imply Future Costs

- Legacy systems and data are one of the largest sources of security vulnerabilities
- Fixing them now is expensive and time-consuming…
  but fixing them later is much worse
  - Systems get even older and less supported
  - Harder to find talent
  - Cyberattacks are devastating to consumers and businesses …
    the worst time to have to deal with legacy systems is in their aftermath

- These risks and costs are already present and should be addressed in evaluation of insurers' financial condition
- Suggest market examinations require that all licensed insurers meet criteria for buying cyber-insurance

- Best time to bring control is now
- Good data privacy regulations should incentivize this

Benefits of Addressing Legacy Systems Proactively

- Data remains a key part of insurers operations and assets
- Modernizing and consolidating data and systems enables:
  - Analytics & data science
  - Better understanding of customers
  - More streamlined and responsive operations
- Being prepared for forthcoming data privacy regulations in at state, federal, global level
  - Meta (Facebook) has had to invest over 800 engineer-years to meet data privacy regulations in EU and elsewhere

Learnings from HIPAA

HIPAA

- US's earliest and most broadly implemented privacy law (1996)
- Much of this NAIC Model Law conceptually parallels HIPAA

Adopting HIPAA took work but was doable

- Health insurers were not bankrupted
- Covered entities underwent big organizational process and culture changes
- Holding covered entities accountable for actions of subcontractors ("business associates") is critical
- Health insurers are now (rightfully) concerned about uncontrolled disclosures
    - E.g insurers were very upset by federal rules permitting app developers to access data without a business associate agreement

Similar activities for compliance with this model

- Same organizational processes for most legal frameworks
- Most state laws in earlier presentation exempted activities covered under HIPAA and other laws

Some Questions for Regulators

- How will insurers show regulators that they have brought legacy systems and data under control?
- How to deal with cases where data cannot be retrieved or accounted for?
- How to account for insurers costs related to legacy systems without unfair and unpredictable premium and market impacts?

Summary

- Consumers are concerned about privacy and handling of their data
- Legacy systems pose significant risks to consumers, insurers, and regulators
- Costs and risks are already present, but are likely not well accounted for in financial examinations
- Getting control of legacy systems and data is key to meeting consumers' expectations of data privacy
- Prior experience with HIPAA shows that regulatory oversight will incur costs but ultimately improve insurers' ability to meet the data privacy standards consumers expect