Public Comments
Privacy of Consumer Financial and Health Information Regulation (#672)

Article VII – Rules for Health Information

Table of Contents

REGULATOR COMMENTS:

Department of Insurance and Financial Services (DIFS) - Michigan

ARTICLE VII. RULES FOR HEALTH INFORMATION

Section 2218. When Authorization Required for Disclosure of Nonpublic Personal Health Information

A. A licensee shall not disclose nonpublic personal health information about a consumer or customer unless an authorization is obtained from the consumer or customer whose nonpublic personal health information is sought to be disclosed.

B. Nothing in this section shall prohibit, restrict or require an authorization for the disclosure of nonpublic personal health information by a licensee for the performance of the following insurance functions by or on behalf of the licensee:

1) claims administration, ~~; claims~~ adjustment, and management;
2) detection, investigation or reporting of actual or potential fraud, misrepresentation or criminal activity;
3) underwriting; policy placement or issuance;
4) loss control;
5) ratemaking and guaranty fund functions;
6) reinsurance and excess loss insurance;
7) risk, case, or disease management;
8) ~~case management; disease management;~~
9) quality assurance~~; quality~~ or improvement;
10) performance evaluation;
11) provider credentialing verification;
12) utilization or ~~review;~~ peer review activities;
13) actuarial, scientific, medical or public policy research;
14) grievance procedures;
15) internal administration of compliance, managerial, and information systems;
16) policyholder service functions;
17) auditing;
18) reporting;
19) database security;
20) administration of consumer disputes and inquiries;
21) external accreditation standards;
22) the replacement of a group benefit plan or workers compensation policy or program;
23) activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit;
24) any activity that permits disclosure without authorization pursuant to the federal Health Insurance Portability and Accountability Act privacy rules promulgated by the U.S. Department of Health and Human Services;
25) disclosure that is required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out a transaction or providing a product or service that a consumer requests or authorizes; and

Commented [ES1]: Would this be encompassed by #26. If so, could this part be removed?

26) any activity otherwise permitted by law, required pursuant to governmental reporting authority, or to comply with legal process.

C. Additional insurance functions may be added with the approval of the commissioner to the extent they are necessary for appropriate performance of insurance functions and are fair and reasonable to the interest of consumers.

Commented [ES2]: This is impossible to read. I propose breaking this section down as noted.

Section 2321~~9~~. Authorizations

A. A valid authorization to disclose nonpublic personal health information pursuant to this Article VII shall be in written or electronic form and shall contain all of the following:

(1) The identity of the consumer or customer who is the subject of the nonpublic personal health information;

(2) A general description of the types of nonpublic personal health information to be disclosed;

(3) General descriptions of the parties to whom the licensee discloses nonpublic personal health information, the purpose of the disclosure and how the information will be used;

(4) The signature of the consumer or customer who is the subject of the nonpublic personal health information or the individual who is legally empowered to grant authority and the date signed; and

(5) Notice of the length of time for which the authorization is valid and that the consumer or customer may revoke the authorization at any time and the procedure for making a revocation.

B. An authorization for the purposes of this Article VII shall specify a length of time for which the authorization shall remain valid, which in no event shall be for more than twenty-four (24) months.

C. A consumer or customer who is the subject of nonpublic personal health information may revoke an authorization provided pursuant to this Article VII at any time, subject to the rights of an individual who acted in reliance on the authorization prior to notice of the revocation.

D. ~~D.~~ A licensee shall retain the authorization or a copy thereof in the record of the individual who is the subject of nonpublic personal health information.

Commented [ES3]: I don't see a provision that states the consumer/customer must be provided a copy of the authorization. I added a provision to that effect.

E. The original authorization or a copy thereof shall be provided to the consumer or customer after the authorization is signed by the consumer or customer.

Section 2~~4~~0. Authorization Request Delivery

A request for authorization and an authorization form may be delivered to a consumer or a customer as part of an opt-out notice pursuant to Section 1~~5~~1, provided that the request and the authorization form are clear and conspicuous. An authorization form is not required to be delivered to the consumer or customer or included in any other notices unless the licensee intends to disclose protected health information pursuant to Section 22~~1~~8A.

Section 251. Relationship to Federal Rules

A Licensee that is subject to and governed by the privacy, security, and breach notification ~~rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, HITECH),~~ under any federal law or rule and that maintains nonpublic personal information in the same manner as protected health information shall be deemed to comply with the requirements of this Act.

This act shall not apply to a nonprofit organization that processes or shares personal information solely for the purposes of assisting law enforcement organizations in investigating criminal or fraudulent acts relating to insurance.~~Irrespective 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.~~

~~**Drafting Note:** The drafters note that the effective date of this regulation is July 1, 2001. The HHS regulation is anticipated to be promulgated in late 2000, thereby becoming effective in late 2002. As of July 1, 2001, if the licensee is in compliance with all requirements of the HHS regulation except its effective date provision, the licensee is not subject to the provisions of this article. If the licensee comes into compliance with the HHS regulation after that date, the licensee is no longer subject to the provisions of this article as of the date the licensee comes into compliance with the HHS regulation.~~

Section 262. Relationship to State Laws

Nothing in this article shall preempt or ~~supercede~~supersede existing state law related to medical records, health or insurance information privacy.

Commented [ES4]: Proposed amendment to include broader language to include any federal law unintentionally omitted from this list and avoid the need for future amendments due to changes in federal law.

Virginia Bureau of Insurance:

The Bureau supports the proposed language found in Article VII setting forth the rules for health information. The Bureau provides suggested edits on the relationship of the rules to other state laws to clarify the scope of the model being drafted. The Bureau offers these edits and comments for the Working Group's consideration and looks forward to continuing to engage with the Working Group this year on this important project.

ARTICLE VII. RULES FOR HEALTH INFORMATION

Section 22. When Authorization Required for Disclosure of Nonpublic Personal Health Information

A. A licensee shall not disclose nonpublic personal health information about a consumer or customer unless an authorization is obtained from the consumer or customer whose nonpublic personal health information is sought to be disclosed.

B. Nothing in this section shall prohibit, restrict or require an authorization for the disclosure of nonpublic personal health information by a licensee for the performance of the following insurance functions by or on behalf of the licensee: claims administration; claims adjustment and management; detection, investigation or reporting of actual or potential fraud, misrepresentation or criminal activity; underwriting; policy placement or issuance; loss control; ratemaking and guaranty fund functions; reinsurance and excess loss insurance; risk management; case management; disease management; quality assurance; quality improvement; performance evaluation; provider credentialing verification; utilization review; peer review activities; actuarial, scientific, medical or public policy research; grievance procedures; internal administration of compliance, managerial, and information systems; policyholder service functions; auditing; reporting; database security; administration of consumer disputes and inquiries; external accreditation standards; the replacement of a group benefit plan or workers compensation policy or program; activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit; any activity that permits disclosure without authorization pursuant to the federal Health Insurance Portability and Accountability Act privacy rules promulgated by the U.S. Department of Health and Human Services; disclosure that is required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out a transaction or providing a product or service that a consumer requests or authorizes; and any activity otherwise permitted by law, required pursuant to governmental reporting authority, or to comply with legal process. Additional insurance functions may be added with the approval of the commissioner to the extent they are necessary for appropriate performance of insurance functions and are fair and reasonable to the interest of consumers.

Section 23. Authorizations

A. A valid authorization to disclose nonpublic personal health information pursuant to this Article VII shall be in written or electronic form and shall contain all of the following:

(1) The identity of the consumer or customer who is the subject of the nonpublic personal health information;

(2) A general description of the types of nonpublic personal health information to be disclosed;

(3) General descriptions of the parties to whom the licensee discloses nonpublic personal health information, the purpose of the disclosure and how the information will be used;

(4) The signature of the consumer or customer who is the subject of the nonpublic personal health information or the individual who is legally empowered to grant authority and the date signed; and

(5) Notice of the length of time for which the authorization is valid and that the consumer or customer may revoke the authorization at any time and the procedure for making a revocation.

B. An authorization for the purposes of this Article VII shall specify a length of time for which the authorization shall remain valid, which in no event shall be for more than twenty-four (24) months.

C. A consumer or customer who is the subject of nonpublic personal health information may revoke an authorization provided pursuant to this Article VII at any time, subject to the rights of an individual who acted in reliance on the authorization prior to notice of the revocation.

D. A licensee shall retain the authorization or a copy thereof in the record of the individual who is the subject of nonpublic personal health information.

Section 24. Authorization Request Delivery

A request for authorization and an authorization form may be delivered to a consumer or a customer as part of an opt-out notice pursuant to Section 15, provided that the request and the authorization form are clear and conspicuous. An authorization form is not required to be delivered to the consumer or customer or included in any other notices unless the licensee intends to disclose protected health information pursuant to Section 22A.

Section 25. Relationship to Federal Rules

A Licensee that is subject to and governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, HITECH), and that maintains nonpublic personal information in the same manner as protected health information shall be deemed to comply with the requirements of this Act.

This act shall not apply to a nonprofit organization that processes or shares personal information solely for the purposes of assisting law enforcement organizations in investigating criminal or fraudulent acts relating to insurance.

Section 26. Relationship to State Laws

Nothing in this article shall preempt or supercede ~~existing~~ state law related to medical records or, health ~~or insurance~~ information privacy.

INDUSTRY COMMENTS:

American Council of Life Insurers (ACLI):

RE: ACLI Comments to Article VII of the Chair's Draft to the Privacy Protections (H) Working Group

Dear Chair Dwyer and Vice Chairs Houdek and Cornelius:

Thank you for the opportunity to provide comments on Article VII of the Chair's Draft revisions to Model 672, pertaining to Rules for Health Information. The continued ability to provide stakeholder input is crucial to ensuring an adoptable revised Model 672 which offers consumers continued and enhanced protections with relation to their data. The suggested comments and redlines below demonstrate further areas to develop uniformity to better consumer understanding across jurisdictions and workability to better effectuate services for consumers and consumer access to products.

While we have appreciated the opportunity to provide specific comments on Article VII, we also wanted to note the following key considerations:

A comprehensive draft of the Model 672 revisions to date would unite regulator, consumer, and all stakeholder understanding in providing comments and improvements to the remaining Articles. The current approach to providing standalone sections of the Chair's draft contains a substantial room for error for stakeholders in preparing feedback for the overarching Chair's Draft as well as the Definitions section. A more cohesive understanding of which sections have been moved where, how sections and articles are situated with one another, and a one-document draft to date for stakeholders and regulators to review would provide a more holistic understanding of where the Draft stands to date and would be very appreciated.

Sufficient time to understand the revisions to the Chair's Draft in context with Definitions will be necessary to ensure the time and effort of the work thus far results in an adoptable Model which will enhance consumer protection. As we diligently participate in this process, we hope to provide the most comprehensive comments on the final revised draft which reflect our expertise and understanding of how to effectuate consumer services and provide readily accessible and available products. These key goals should be considered in establishing a timeline for the completion of this revision effort.

ACLI's Suggested Redlines and Comments

In Section 22(B), we suggest striking "by or on behalf of the licensee" to better address group plans. This qualifier, in practice, is unnecessarily limiting. For example, a licensee cannot share nonpublic personal health information with a group insurance customer for the customer's own plan administration purposes, or the customer's own investigative purposes. Many companies routinely receive requests from group customers for information regarding their customer's plan purposes and are then limited by whether the company has obtained specific individual authorizations. While companies seek these authorizations as part of their claim processes, in practice this information is not regularly received which leads to a disjointed plan administration experience for group customers.

Further in Section 22(B), we suggest adding language to address processing, investigation, and evaluations to fully encompass the scope of existing performance functions on behalf of consumers. The consumer expectation that products and services can be effectuated in a timely and accessible manner relies upon the ability of licensees to maintain current business practices reflected in our suggested edits.

Clarification on the inclusion in Section 25 Relationship to Federal Rules of "This act shall not apply to a nonprofit organization that processes or shares personal information solely for the purposes of assisting law enforcement organizations in investigating criminal or fraudulent acts relating to insurance," would be helpful in understanding the context for this addition. We would appreciate any further information on why the inclusion of this statement is necessary or the intention of including this statement to better understand how to provide comments.

In Section 25, we also seek clarification on the deletion of the Drafting Note. Was it the drafting intention to remove this note as a substantive change or rather a cleanup of the Model to simplify language? In order to maintain protections across life and other long-term policies, we would suggest keeping the note in the absence of a substantial benefit to deletion.

ACLI Suggested Redlines to Article VII Chair's Draft

ARTICLE VII. RULES FOR HEALTH INFORMATION

Section 22. When Authorization Required for Disclosure of Nonpublic Personal Health Information

A. A licensee shall not disclose nonpublic personal health information about a consumer or customer unless an authorization is obtained from the consumer or customer whose nonpublic personal health information is sought to be disclosed.

B. Nothing in this section shall prohibit, restrict or require an authorization for the disclosure of nonpublic personal health information by a licensee for the performance of the following insurance functions ~~by or on behalf of the licensee~~: claims administration and processing; claims investigation, evaluation, adjustment and management; detection, investigation or reporting of actual or potential fraud, misrepresentation or criminal activity; underwriting; policy placement or issuance; loss control; ratemaking and guaranty fund functions; reinsurance and excess loss insurance; risk management; case management; disease management; quality assurance; quality improvement; performance evaluation; provider credentialing verification; utilization review; peer review activities; actuarial, scientific, medical or public policy research; grievance procedures; internal administration of compliance, managerial, and information systems; policyholder service functions; auditing; reporting; database security; administration of consumer disputes and inquiries; external accreditation standards; the replacement of a group benefit plan or workers compensation policy or program; activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit; any activity that permits disclosure without authorization pursuant to the federal Health Insurance Portability and Accountability Act privacy rules promulgated by the U.S. Department of Health and Human Services; disclosure that is required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out a transaction or providing a product or service that a consumer requests or authorizes; and any activity otherwise permitted by law, required pursuant to governmental reporting authority, or to comply with legal process. Additional insurance functions may be added with the approval of the commissioner to the extent they are necessary for appropriate performance of insurance functions and are fair and reasonable to the interest of consumers.

Section 23. Authorizations

A. A valid authorization to disclose nonpublic personal health information pursuant to this Article VII shall be in written or electronic form and shall contain all of the following:

(1) The identity of the consumer or customer who is the subject of the nonpublic personal health information;

(2) A general description of the types of nonpublic personal health information to be disclosed;

(3) General descriptions of the parties to whom the licensee discloses nonpublic personal health information, the purpose of the disclosure and how the information will be used;

(4) The signature of the consumer or customer who is the subject of the nonpublic personal health information or the individual who is legally empowered to grant authority and the date signed; and

(5) Notice of the length of time for which the authorization is valid and that the consumer or customer may revoke the authorization at any time and the procedure for making a revocation.

B. An authorization for the purposes of this Article VII shall specify a length of time for which the authorization shall remain valid, which in no event shall be for more than twenty-four (24) months.

C. A consumer or customer who is the subject of nonpublic personal health information may revoke an authorization provided pursuant to this Article VII at any time, subject to the rights of an individual who acted in reliance on the authorization prior to notice of the revocation.

D. A licensee shall retain the authorization or a copy thereof in the record of the individual who is the subject of nonpublic personal health information.

Section 24. Authorization Request Delivery

A request for authorization and an authorization form may be delivered to a consumer or a customer as part of an opt-out notice pursuant to Section 15, provided that the request and the authorization form are clear and conspicuous. An authorization form is not required to be delivered to the consumer or customer or included in any other notices unless the licensee intends to disclose protected health information pursuant to Section 22A.

Section 25. Relationship to Federal Rules

A Licensee that is subject to and governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, HITECH), and that maintains nonpublic personal information in the same manner as protected health information shall be deemed to comply with the requirements of this Act.

This act shall not apply to a nonprofit organization that processes or shares personal information solely for the purposes of assisting law enforcement organizations in investigating criminal or fraudulent acts relating to insurance.

ACLI Seeks to better understand the inclusion of the highlighted sentence above.

ACLI seeks to better understand the deletion of the Drafting Note, previously stating: "Drafting Note: The drafters note that the effective date of this regulation is July 1, 2001. The HHS regulation is anticipated to be promulgated in late 2000, thereby becoming effective in late 2002. As of July 1, 2001, if the licensee is in compliance with all requirements of the HHS regulation except its effective date provision, the licensee is not subject to the provisions of this article. If the licensee comes into compliance with the HHS regulation after that date, the licensee is no longer subject to the provisions of this article as of the date the licensee comes into compliance with the HHS regulation."

Section 26. Relationship to State Laws

Nothing in this article shall preempt or supercede existing state law related to medical records, health or insurance information privacy.

American Property Casualty Insurance Association (APCIA):

RE: *APCIA Comments on Article VII- Rules for Health Information*

Dear Chair Dwyer and Members of the Privacy Protections (H) Working Group:

Thank you for the opportunity to submit comments on Article VII of the Privacy Protections Working Group's Chair Draft revising the Privacy of Consumer Financial and Health Information Regulation (Model #672). APCIA[1] appreciates the Working Group's continued efforts to modernize the insurance-specific privacy framework and its thoughtful engagement throughout this process.

Given the absence of a complete redraft showing all interrelated provisions and definitions together, our comments are necessarily caveated. Reviewing individual articles in isolation makes it difficult to assess the full context, cumulative impact, and interaction among provisions, particularly where key terms remain undefined.

Based on our review of Article VII as currently drafted, we do not identify concerns at this time. However, as the broader draft evolves and definitions and related provisions are finalized, we may provide additional feedback.

We respectfully encourage the Working Group to provide a longer review period when the full draft is re-exposed to ensure stakeholders have adequate opportunity to evaluate the complex interplay of provisions and support a meaningful and workable modernization of this important framework.

National Association of Mutual Insurance Companies (NAMIC):

ARTICLE VII. RULES FOR HEALTH INFORMATION

Section 22. When Authorization Required for Disclosure of Nonpublic Personal Health Information

A. A licensee shall not disclose nonpublic personal health information about a consumer or customer unless an authorization is obtained from the consumer or customer whose nonpublic personal health information is sought to be disclosed.

B. Nothing in this section shall prohibit, restrict or require an authorization for the disclosure of nonpublic personal health information by a licensee for the performance of the following insurance functions by or on behalf of the licensee: claims administration and processing; claims investigation, evaluation, adjustment and management; detection, investigation or reporting of actual or potential fraud, misrepresentation or criminal activity; underwriting; policy placement or issuance; loss control; ratemaking and guaranty fund functions; reinsurance and excess loss insurance; risk management; case management; disease management; quality assurance; quality improvement; performance evaluation; provider credentialing verification; utilization review; peer review activities; actuarial, scientific, medical or public policy research; grievance procedures; internal administration of compliance, managerial, and information systems; policyholder service functions; auditing; reporting; database security; administration of consumer disputes and inquiries; external accreditation standards; the replacement of a group benefit plan or workers compensation policy or program; activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit; any activity that permits disclosure without authorization pursuant to the federal Health Insurance Portability and Accountability Act privacy rules promulgated by the U.S. Department of Health and Human Services; disclosure that is required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out a transaction or providing a product or service that a consumer requests or authorizes; and any activity otherwise permitted by law, required pursuant to governmental reporting authority, or to comply with legal process. Additional insurance functions may be added with the approval of the commissioner to the extent they are necessary for appropriate performance of insurance functions and are fair and reasonable to the interest of consumers.

Commented [LS5]: NAMIC suggests that the general references to claims administration, adjustment, or management may be broad enough to address subrogation claims. However, to make it clearer, we suggest the working group specifically mention subrogation here as well.

Section 232. Authorizations

A. A valid authorization to disclose nonpublic personal health information pursuant to this Article VII shall be in written or electronic form and shall contain all of the following:

(1) The identity of the consumer or customer who is the subject of the nonpublic personal health information;

(2) A general description of the types of nonpublic personal health information to be disclosed;

(3) General descriptions of the parties to whom the licensee discloses nonpublic personal health information, the purpose of the disclosure and how the information will be used;

(4) The signature of the consumer or customer who is the subject of the nonpublic personal health information or the individual who is legally empowered to grant authority and the date signed; and

(5) Notice of the length of time for which the authorization is valid and that the consumer or customer may revoke the authorization at any time and the procedure for making a revocation.

B. An authorization for the purposes of this Article VII shall specify a length of time for which the authorization shall remain valid, which in no event shall be for more than twenty-four (24) months.

C. A consumer or customer who is the subject of nonpublic personal health information may revoke an authorization provided pursuant to this Article VII at any time, subject to the rights of an individual who acted in reliance on the authorization prior to notice of the revocation.

Commented [LS6]: The current scope here is limited to written or electronic forms of authorization; NAMIC suggests the working group also consider or contemplate verbal authorization (i.e., over the phone or that given in person from the consumer).

Commented [LS7]: The limitation of 24 months here with revocation rights could result in complications for P&C carriers with respect to data management.

For instance, P&C carriers may need to implement new processes to:

- Obtain valid authorizations before disclosing health-related data.
- Track expiration and revocation of authorizations.
- Maintain records of authorizations securely.

All of these factors can impose operational and compliance costs, especially for carriers that share health-related information with third parties (e.g., medical providers, investigators).

Currently, med authorization has no expiration but is valid until revocation.

Commented [LS8]: NAMIC requests additional clarification in paragraph C in the way of what constitutes "reliance."

D. A licensee shall retain the authorization or a copy thereof in the record of the individual who is the subject of nonpublic personal health information.

Section 24. Authorization Request Delivery

A request for authorization and an authorization form may be delivered to a consumer or a customer as part of an opt-out notice pursuant to Section 15, provided that the request and the authorization form are clear and conspicuous. An authorization form is not required to be delivered to the consumer or customer or included in any other notices unless the licensee intends to disclose protected health information pursuant to Section 22A.

Section 25. Relationship to Federal Rules

A Licensee that is subject to and governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, HITECH), and that maintains nonpublic personal information in the same manner as protected health information shall be deemed to comply with the requirements of this Act.

This act shall not apply to a nonprofit organization that processes or shares personal information solely for the purposes of assisting law enforcement organizations in investigating criminal or fraudulent acts relating to insurance.

Section 26. Relationship to State Laws

Nothing in this article shall preempt or supersede existing state law related to medical records, health or insurance information privacy.

Commented [LS9]: NAMIC puts forth the following questions for the Working Group to consider and provide clarity on:

1.What does the Working Group intend by "maintain"?

2.To meet the safe harbor proposed here, would insurers need to also follow similar breach standards, and de-identified HIPAA standards? Does the Working Group contemplate also requiring that the insurer have Business Associate Agreements in place to meet the safe harbor?

Commented [LS10]: NAMIC posits that inclusion of this provision results in creating a complex patchwork of requirements, increasing compliance complexity and costs for carriers operating in multiple jurisdictions, because carriers would need to comply not only with this Act, but with any existing or further state laws on health or insurance information privacy.

CONSUMER REPRESENTATIVE:

FROM THE NAIC CONSUMER REPRESENTATIVES

TO: NAIC Privacy Protections (H) Working Group
sent via email to: privacywg@naic.org

DATE: March 9, 2026

RE: **Comments on PPWG Chair Draft Article VII**

Thank you to the Privacy Protections (H) Working Group for the opportunity to continue to comment on the privacy model act that the Working Group is drafting. Attached is a WORD document with our recommendations for revisions in red and highlighted in yellow. In addition, please also refer to the Comments in the margin of this submission.

Should you have any questions about this document, feel free to contact Harry Ting or one of the other NAIC Consumer Representatives signees below.

Signed by NAIC Consumer Representatives

Brenda Cude
Brendan Bridgeland
Brent Walker
Claire Heyison
Harold Ting
Kenneth Klein
Peter Kochenberger
Richard Weber
Silvia Yee

ARTICLE VII. RULES FOR HEALTH INFORMATION

Section 22. When Authorization Required for Disclosure of Nonpublic Personal Health Information

A. A licensee shall not disclose nonpublic personal health information about a consumer or customer unless an authorization is obtained from the consumer or customer whose nonpublic personal health information is sought to be disclosed.

B. Nothing in this section shall prohibit, restrict or require an authorization for the disclosure of nonpublic personal health information by a licensee for the performance of the following insurance functions by or on behalf of the licensee:

(1) Claims administration; claims adjustment and management; detection, investigation or reporting of actual or potential fraud, misrepresentation or criminal activity; underwriting; policy placement or issuance; loss control; ratemaking and guaranty fund functions; reinsurance and excess loss insurance; risk management; case management; disease management; quality assurance; quality improvement; performance evaluation; provider credentialing verification; utilization review; peer review activities; ~~actuarial, scientific, medical or public policy research;~~ grievance procedures; internal administration of compliance, managerial, and information systems; policyholder service functions; auditing; reporting; database security; administration of consumer disputes and inquiries; ~~external accreditation standards; the replacement of a group benefit plan or workers compensation policy or program; activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit;~~

(2) Activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit;

(3) Any activity that permits disclosure without authorization pursuant to the federal Health Insurance Portability and Accountability Act privacy rules promulgated by the U.S. Department of Health and Human Services and other applicable laws;

(4) Disclosure that is required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out a transaction or providing a product or service that a consumer requests or authorizes; and any activity otherwise permitted by law, required pursuant to governmental reporting authority, or to comply with legal process. ~~Additional insurance functions may be added with the approval of the commissioner to the extent they are necessary for appropriate performance of insurance functions and are fair and reasonable to the interest of consumers.~~

C. Nonpublic personal health information shall not be shared for use in actuarial, scientific, medical or public policy research, unless the data has been anonymized, so that individuals associated with the nonpublic personal health information cannot be identified.

Commented [CR11]: Activities included in this revised Section 22.B(1) seem to be ones that are covered by HIPAA. Would it make sense to just replace this by referring to activities permitted by HIPAA?

Commented [CR12]: HIPAA sets a floor on privacy protections. It frequently will permit a disclosure without authorization that other privacy laws - the federal substance use disorder confidentiality regs (42 CFR Part 2) or state privacy laws for HIV, mental health and reproductive health prohibit.

Section 23. Authorizations

A. A valid authorization to disclose nonpublic personal health information pursuant to this Article VII shall be in written or electronic form and shall contain all of the following:

(1) The identity of the consumer or customer who is the subject of the nonpublic personal health information;

(2) A ~~general~~ specific and meaningful description of the types of nonpublic personal health information to be disclosed;

(3) General descriptions of the parties to whom the licensee discloses nonpublic personal health information, the purpose of the disclosure and how the information will be used;

(4) The signature of the consumer or customer who is the subject of the nonpublic personal health information or the individual who is legally empowered to grant authority and the date signed; and

(5) Notice of the length of time for which the authorization is valid and that the consumer or customer may revoke the authorization at any time and the procedure for making a revocation.

(6) A description of the purpose of the requested disclosure.

(7) Any additional information required to comply with HIPAA and any other applicable law, including the federal confidentiality protections for substance use disorder treatment records (42 USC Section 290dd-2 and 42 CFR Part 2) as well as state laws.

B. An authorization for the purposes of this Article VII shall specify a length of time for which the authorization shall remain valid, which in no event shall be for more than twenty-four (24) months.

C. A consumer or customer who is the subject of nonpublic personal health information may revoke an authorization provided pursuant to this Article VII at any time, subject to the rights of an individual who acted in reliance on the authorization prior to notice of the revocation.

D. A licensee shall retain the authorization or a copy thereof in the record of the individual who is the subject of nonpublic personal health information.

Section 24. Authorization Request Delivery

A request for authorization and an authorization form may be delivered to a consumer or a customer as part of an opt-out notice pursuant to Section 15, provided that the request and the authorization form are clear and conspicuous. An authorization form is not required to be delivered to the consumer or customer or included in any other notices unless the licensee intends to disclose protected health information pursuant to Section 22A.

Section 25. Relationship to Federal Rules

Nothing in this Article shall preempt or supersede existing federal laws that affect Licensees ~~that~~ ~~is~~ subject to and governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the

Commented [CR13]: HIPAA and 42 CFR Part 2 require the purpose to be "specific and meaningful"

Commented [CR14]: Compliance with HIPAA should not be deemed to comply with Article VII, because licensees may have nonpublic personal health information that is not covered by HIPAA (e.g., health data purchased from data brokers or data from sellers of health-related products or services). Furthermore, many licensees are not covered by HIPAA.

Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), ~~and~~ the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, HITECH) or Part 2 of Title 42 the Code of Federal Regulations. ~~that maintains nonpublic personal information in the same manner as protected health information~~

~~This act shall not apply to a nonprofit organization that processes or shares personal information solely for the purposes of assisting law enforcement organizations in investigating criminal or fraudulent acts relating to insurance.~~ This act shall not apply to the National Association of Insurance Commissioners and the National Insurance Crime Bureau when processing or sharing information solely for the purposes of investigating criminal or fraudulent insurance acts.

Section 26. Relationship to State Laws

Nothing in this article shall preempt or ~~supercedes~~supersede existing state law related to medical records, consumer data privacy, or health or insurance information privacy.

Commented [CR15]: Part 2 of Title 42 imposes tigher rrestrictions on the sharing of substance abuse PHI than HIPAA does.

Commented [CR16]: This change reflects a concern that if all nonprofit organizations are exempted, that some with a political agenda may use this exemption to investigate what they consider to be "undesirable" activities of consumers.