NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

Date: 6/10/21

PRIVACY PROTECTIONS (D) WORKING GROUP
Monday, June 14, 2021
3:15–4:45 pm Eastern / 2:15–3:45 pm Central / 1:15–2:45 pm Mountain / 12:15–1:45 pm Pacific

ROLL CALL

Cynthia Amann, Chair	Missouri	Martin Swanson	Nebraska
Ron Kreiter, Vice Chair	Kentucky	Chris Aufenthie/Johnny Palsgraaf	North Dakota
Damon Diederich	California	Teresa Green	Oklahoma
Erica Weyhenmeyer	Illinois	Raven Collins/Brian Fordham	Oregon
LeAnn Crow	Kansas	Gary Jones	Pennsylvania
T.J. Patton	Minnesota	Don Beatty/Katie Johnson	Virginia
Molly Plummer/Tyler Spady	Montana		

NAIC Support Staff: Lois E. Alexander/Greg Welker

AGENDA

1. Consider Adoption of its May 10 Minutes—*Cynthia Amann (MO)* — Attachment A

2. Discuss Comments Received on the Initial Privacy Policy Statement —*Cynthia Amann (MO)* — Attachments B, C, and D
   - Robert Ridgeway, Americas Health Insurance Plans-AHIP
   - Randi Chapman and Lauren Choi, Blue Cross Blue Shield Association-BCBSA
   - Chris Petersen, Arbor Strategies LLC/Coalition of Health Insurers

3. Discuss Any Other Matters Brought Before the Working Group —*Cynthia Amann (MO)*

4. Adjournment—*Cynthia Amann (MO)*

W:\National Meetings\2021\Summer\Cmte\D\Privacy Protections\June 14 Call\061421_PPWG Agenda.Docx

Draft: 6/10/21

Privacy Protections (D) Working Group
Virtual Meeting
May 10, 2021

The Privacy Protections (D) Working Group of the Market Regulation and Consumer Affairs (D) Committee met May 10, 2021. The following Working Group members participated: Cynthia Amann, Chair, (MO); Ron Kreiter, Vice Chair (KY); LeAnn Crow (KS); T.J. Patton (MN); Chris Aufenthie and Johnny Palsgraaf (ND); Martin Swanson (NE); Teresa Green (OK); Gary Jones (PA); and Don Beatty and Katie Johnson (VA).

1. Adopted its March 29 Minutes

The Working Group met March 29 and took the following action: 1) adopts its 2020 Fall National Meeting minutes; 2) receive status reports on federal and state privacy legislation; 3) review the 2021 NAIC Member-Adopted Strategy for Consumer Data Privacy Protections; 4) discuss comments received on the 2020 Fall National Meeting verbal gap analysis; and 5) announce the Consumer Privacy Protections Panel at the NAIC Virtual Insurance Summit.

Mr. Beatty made a motion, seconded by Mr. Swanson, to adopt the Working Group's March 29 minutes (Attachment A). The motion passed unanimously.

2. Discussed the Draft of the Initial Privacy Policy Statement

Ms. Amann said the Working Group completed its work plan in 2020. She said the Working Group received additional guidance through the Market Regulation and Consumer Affairs (D) Committee in the form of the following NAIC Member-Adopted Strategy for Consumer Data Privacy Protections (Attachment D). She said the Working Group is currently working on item C because item A and item B have already been completed.

NAIC Member-Adopted Strategy for Consumer Data Privacy Protections

1. Charge the Market Regulation and Consumer Affairs (D) Committee with:
   a. Summarizing consumer data privacy protections found in existing NAIC models—the *Health Information Privacy Model Act* (#55), the *NAIC Insurance Information and Privacy Protection Model Act* (#670), and the *Privacy of Consumer Financial and Health Information Regulation* (#672).
   b. Identifying notice requirements of states, the European Union's (EU's) General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), and how insurers may be subject to these requirements.
   c. Identifying corresponding consumer rights that attach to notice requirements, such as the right to opt-out of data sharing, the right to correct or delete information, the right of data portability and the right to restrict the use of data, and how insurers may be subject to these requirements.
   d. Setting forth a policy statement on the minimum consumer data privacy protections that are appropriate for the business of insurance.
   e. Delivering a report on items (a– d) above by the NAIC Fall National Meeting.
2. Engage with state attorneys general (AGs), Congress and federal regulatory agencies on state and federal data privacy laws to minimize preemption provisions and maximize state insurance regulatory authority.
3. Reappoint the Privacy Protections (D) Working Group to revise NAIC models, as necessary, to incorporate minimum consumer data privacy protections that are appropriate for the business of insurance. Complete by the NAIC Fall National Meeting.

Ms. Amann said Minnesota, Nevada, Oregon, and Virginia submitted comments on the initial privacy policy statement drafted in accordance with item D as a framework on which to build minimum consumer data privacy protections that are appropriate for the business of insurance. She said states on the state insurance regulator subject matter expert (SME) group agreed that all six categories identified in the statement should stay. Ms. Johnson said Virginia might be including portability in its Uniform Electronic Transactions Act (UETA), as Virginia said a consumer had to opt-in, meaning that companies could post a disclosure online, but the company must mail the disclosure to the consumer if the consumer asks for a hard copy of the document. Mr. Beatty asked Brooke Stringer (NAIC) if the categories listed were sufficient to address federal issues, topics, and concerns. Ms. Stringer said preemption and private rights of action are two of the top federal issues, so she said the categories identified are within the realm of federal expectations. Mr. Patton asked how consumers could opt-in and opt-out, as these two categories seem to be opposites. Ms. Amann said the Working Group's approach right now would be to consider both and recommend

one following its discussions. Mr. Patton said the chart should be updated, as Minnesota did address the bill listed even though the bill did not move.

Chris Petersen (Arbor Strategies LLC), speaking on behalf of the Coalition of Health Insurers, said general statements, such as those in the *Unfair Trade Practices Act* (#880), require companies only to maintain records. He said if the right to delete is allowed, it would be impossible for the company to maintain those records. He said the Health Insurance Portability and Accountability Act (HIPAA) only allowed the right to request, not to delete. He also said adding examples to recommendations would be helpful as guidance. Ms. Amann said the six categories will serve as the topics to be discussed at a high level, and examples would be a good idea. She said verbiage would be drafted as a point of discussion, as well as perhaps to specify that it is for the insurance sector only. Kate Kiernan (Public Policy Consulting) said in Minnesota, opt-in and opt-out are not mutually exclusive. She said the same law can have opt-in for more sensitive information and opt-out for less sensitive information.

Angela Gleason (American Property Casualty Insurance Associations—APCIA) suggested that the Working Group not discuss already regulated issues. Ms. Amann said this general discussion is for today's call only. She said HIPAA is so controlling that the Working Group may not be able to change or revise it, the Gramm-Leach-Bliley Act (GLBA), etc., so these are to be put aside for now to be folded in later as consumers, industry, and state insurance regulators refine the draft. Bob Ridgeway (Americas Health Insurance Plans—AHIP) asked why Section A of the draft is separate from Section B. Ms. Amann said she envisions: 1) Section A to mean why the consumer has the right to correct with policy reasons in favor of it and why; 2) Section B to mean how an insured could do this, and as a practical matter that the consumer could not correct information fraudulently—i.e., change information that is proven to be true via public records (arrest records, court documents, etc.)—and the right to correct could only be within or after 180 days; and 3) Section C to mean how state insurance regulators would enforce this. Ms. Johnson said states that had adopted Model #670 had accelerated underwriting notice; it says the consumer can correct or delete incorrect information if the company has taken an adverse action, and it has a limitation on timing of the information. Ms. Amann said existing limitations would still apply. She said new recommended revisions would not cover all carte blanche, and the policy statement would help to explain these situations. Mr. Petersen said non-insurance information should not be looked at by the Working Group, but the Working Group should only look at the insurance industry. He said HIPAA's right to request is not absolute. Ms. Johnson said it would be helpful to have information from industry on where the rails should be, and Virginia would only look at information companies gather. Ms. Kiernan asked if the privacy policy statement would be final by the Fall National Meeting. Ms. Amann said it would be final and would recommend if a new model is needed or if revisions would be needed, as well as the parameters for the new model or changes.

Ms. Amann requested comments in the form of parameters and examples on the initial privacy policy statement by June 7 for discussion during the next Working Group meeting scheduled for June 14.

Ms. Alexander said she would attempt to schedule Working Group meetings every four to six weeks, while avoiding overlap with other groups working on interrelated issues.

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

W:\National Meetings\2021\Summer\Cmte\D\Privacy Protections\Privacyprot_05-10_Min.Docx

601 Pennsylvania Avenue, NW
South Building, Suite 500
Washington, D.C. 20004

T 202.778.3200
F 202.331.7487
ahip.org

June 7, 2021

Cynthia Amann, Chair
Privacy Protections (D) Working Group
Missouri Department of Insurance

c/o National Association of Insurance Commissioners
Attn: Lois Alexander, Market Regulation Manager
Via email: LAlexander@NAIC.org

Re: Privacy Protections (D) Working Group – Initial Draft Privacy Policy Statement (April 28, 2021)

Dear Ms. Amann;

On behalf of AHIP's member plans, we welcome the opportunity to comment on the Initial Draft Privacy Policy Statement exposure. We appreciate your patient and measured approach to this complex issue.

You have asked for high-level comments on the six topics outlined in the Initial Draft Privacy Policy Statement.

While our comments represent the health insurers' perspective, it is also important to note that our responses also reflect the views and needs of our members' enrollees. Further, since health insurers' operations in matters including, but not limited to privacy, data security, claims payments, and quality measurement are extensively regulated by the Health Insurance Portability and Accountability Act (HIPAA), the Privacy and Security Rules (45 C.F.R. Parts 160, 164), the Health Information Technology for Economic and Clinical Health ("HITECH") Act (Pub. L. No. 111-5) and the 2020 Interoperability and Patient Access Final Rule (85 FR 25510) ("Interoperability Rule"), most of our comments will refer to existing requirements under those regulations.

Where the Privacy Rule addresses the six topics below, its provisions reflect a careful weighing of numerous competing interests in the unique health care context, as established through an extensive, multi-year rule-making process. The descriptions below are high-level summaries of how the Privacy Rule addresses the topics. The actual regulatory provisions are significantly more detailed.

The right to opt-out of data sharing & the right to opt-in to data sharing. A HIPAA Covered Entity is prohibited from using or disclosing an individual's protected health information unless the information is to be used or disclosed for an allowed purpose such as treatment, payment, or

health care operations or otherwise permitted or required by policy-based exemptions in the Privacy Rule (45 CFR 164.502(a), and 45 CFR 164.508). For these purposes, neither HIPAA nor HITECH mandates either an opt-in or an opt-out approach. An individual's written authorization is required for additional uses or disclosures.

The right to correct information. HIPAA already provides an individual with the right to amend incorrect or inaccurate information. 45 CFR 164.526.

The right to delete information. Ensuring patient safety and the accuracy of clinical decision-making requires a complete record of a patient's history. The record protects not only the patient but also the Covered Entity. As such, there is no specific "right to delete" in HIPAA. However, an individual's right to request that a Covered Entity correct or amend incorrect or inaccurate PHI at 45 CFR 154.526, provides a detailed process for individuals to request amendment of PHI, for Covered Entities to either approve or deny the amendment, and for the exercise of related procedural rights. In addition to the right of amendment, HIPAA provides individuals with the right of access (i.e., to inspect and receive a copy) and the right to an accounting of disclosures of PHI. While a Covered Entity must retain PHI, an individual's rights of access, amendment, and accounting provide important procedural safeguards.

In addition, state laws are replete with records-retention requirements which would, in most if not all cases, directly conflict with most interpretations of a "right to delete." Although the recent California Consumer Protection Act (CCPA) is often cited in support of the "right to delete" or the "right to be forgotten", that right is not absolute, and there are exceptions. Several of those exceptions in the CCPA are based on other regulations. For example, data already regulated by the Gramm-Leach-Bliley Act (GLBA) and HIPAA are not subject to the CCPA. However, some of the exceptions are more generally applicable and, absent further direction from the California Attorney General, open to interpretation. The exceptions apply to information necessary to complete transactions; uphold legal obligations; maintain security and existing functionality; protect free speech; conduct research; and allow for internal, expected, and lawful uses. Cal. Civ. Code Sec. 1798.105

The right of data portability. The Federal privacy statutory and regulatory framework handles portability in two main ways. First, the HIPAA Privacy Rule provides individuals with the right to access and obtain a copy of the protected health information about the individual (45 CFR 164.524). Additionally, an individual has the right to receive an accounting of all disclosures of their information made by a covered entity within the previous six years (45 CFR 164.528). An individual can also direct disclosures to third parties (*e.g*, an attorney in a civil suit) by signing a written authorization for the specific information and the individual or entity to whom the protected health information should be disclosed. See 45 CFR 164.524(cc)(3)(ii). Earlier this year, HHS issued a notice of proposed rulemaking which would further strengthen an

individual's right of access and the right to direct disclosure of PHI to third parties. See 86 FR 6446 (January 21, 2021).

Second, the recent 2020 Interoperability and Patient Access final rule was intended to innovate and streamline how consumers access their medical records from their health insurers in federal programs. The regulation requires the development and use of application programming interfaces (APIs) to seamlessly share electronically protected health information with third-party applications or "apps" for consumers to access their health information to improve their health, monitor their conditions, or other related services. However, we note that this process moves the personally identifiable information outside the reach of HIPAA, potentially leaving the patient's information vulnerable.

The right to restrict the use of data. The HIPAA Privacy Rule provides individuals with the right to request a covered entity to restrict uses or disclosures of their information to carry out treatment, payment, or health care operations, as well as other otherwise permitted disclosures. See 45 CFR 164.522. There are also provisions within HIPAA for "confidential communications" which set out processes for agreed-upon information disclosures.

The paragraphs above touch on only a few ways HIPAA regulates the health insurance industry as well as the broader health care system. Our members have spent years implementing and maintaining compliance with these and other HIPAA-mandated national requirements to ensure our consumers' privacy rights are well-protected. Further, this is a system that is regularly reviewed and improved (e.g., HITECH, and the Interoperability Rule). We urge the Privacy Protections Working Group to preserve these exemptions for insurers subject to HIPAA by avoiding any action that conflicts, challenges, or needlessly duplicates these requirements.

We hope this information is helpful and look forward to discussing it further with you. Please let me know if you have questions in the meantime.

Sincerely,

Bob Ridgeway
America's Health Insurance Plans
Bridgeway@AHIP.org
501-333-2621

BlueCross BlueShield Association

An Association of Independent
Blue Cross and Blue Shield Plans

June 7, 2021

NAIC Privacy Protections (D) Working Group
Attn: Lois Alexander, Market Regulation Manager II
Via email: lalexander@naic.org

RE: Privacy Protections (D) Working Group Policy Statement Exposure Draft

Dear Chair Amann, Vice Chair Kreiter, and Members of the Working Group:

Thank you for the opportunity to provide additional input on the Privacy Protections (D) Working Group's (Working Group) Policy Statement Exposure Draft (Draft Policy Statement). As indicated by the draft, "this initial draft privacy policy statement is the framework for the minimum consumer data privacy protections that are appropriate for the business of insurance to be applied to NAIC model #672 as revisions, if possible, or as a start for a new model, if necessary."

BCBSA is a national federation of 35 independent, community-based and locally operated Blue Cross and Blue Shield companies (Plans) that collectively provide health care coverage for one in three Americans. For more than 90 years, Blue Cross and Blue Shield companies have offered quality health care coverage in all markets across America – serving those who purchase coverage on their own as well as those who obtain coverage through an employer, Medicare and Medicaid.

We laud the Working Group's efforts to initiate a collaborative process to develop this framework. Informed by our experience, we respectfully offer feedback to the Draft Policy Statement. As explained in more detail below, we wish to highlight the following key recommendations:

1. In addition to identifying substantive minimum consumer data privacy protections as is currently laid out in the Draft Policy Statement, the framework should narrow its applicability to specifically exempt health insurers through a "carve-out" provision. Health insurers are already subject to extensive and evolving data privacy protection requirements under the Health Insurance Portability and Accountability Act (HIPAA) and other federal laws.

2. To the extent that health insurers already subject to HIPAA are not exempt from any and all privacy protections developed to be incorporated into NAIC model #672, the model, with respect to health insurers, should conform to HIPAA standards so that consumers remain protected without creating duplicative, confusing and burdensome requirements that add potentially little to no additional consumer protection.

To support these recommendations, additional comments are provided below.

1. **Carve Out Health Insurers as HIPAA-Covered Entities**

HIPAA contains robust existing consumer data privacy protections and continues to evolve to meet the needs of consumers and the technological advances in the health care sector.[1] As covered entities under HIPAA, health insurers are subject to these protections and have implemented physical and administrative safeguards to protect individuals' health information. Deference to HIPAA's regulatory and enforcement regime around consumer data privacy protections is appropriate given the extent to which the health insurance industry must: 1) protect health information when using and disclosing protected health information; 2) only use such information for treatment, payment and health care operations (unless individual authorization is obtained); and 3) adhere to consumer rights standards that have been in place for decades. Therefore, the Draft Policy Statement should include language around scope of applicability to carve out health insurers from any potential consumer data privacy standards that may be applied to NAIC model #672 as revisions (or as a start of a new model). Adding an additional layer of consumer data privacy requirements through an NAIC model update (or new model) would be duplicative, confusing to both consumers and health insurers, and add administrative burden and costs without adding meaningful protections for consumers.

Additional detail explaining how HIPAA requirements already address each of the consumer rights and corresponding notice requirements the Working Group is considering is addressed in the next section. We hope this detail helps the Working Group understand why it is not appropriate to extend model changes to health insurers.

2. **Align Any Additional Model Requirements Applicable to Health Insurers with HIPAA Consumer Data Privacy Protections**

To the extent that the Draft Policy Statement and any eventual model changes extend consumer data privacy requirements to health insurers, such model requirements should not go beyond existing requirements under HIPAA. Alignment with HIPAA will ensure that the same robust privacy protections apply to the same type and use of health information, no matter the jurisdiction. Doing so will mitigate duplication and conflict between federal and state requirements to prevent confusion, potentially differing interpretations, and burden among health insurance industry stakeholders and consumers. The following reference guide addresses how HIPAA regulates health insurer requirements regarding the consumer rights identified in the Draft Policy Statement as well as the notice requirements pertaining to informing consumers of such rights.

- **Right to opt out of data sharing**

  Existing privacy requirements to which health insurers are subject provide significant protections for consumers with respect to data sharing. The HIPAA Privacy Rule imposes stringent requirements. The general rule is that protected health information

[1] An example of how HIPAA continues to evolve is exemplified by the recent proposed regulation published January 21, 2021, entitled, "Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement" which would, among other things, amend an individual's right of access to inspect and obtain copies of personal health information (PHI) and modernize Notice of Privacy Protection Requirements. 86 Fed. Reg. 6446.

(PHI) cannot be used or disclosed by health insurers as covered entities *unless* specifically permitted by federal regulations.[2] HIPAA permits health plans to use and disclose PHI for treatment, payment and health care operations purposes without individual authorization.[3] Generally speaking, any use or disclosure of PHI beyond these purposes must be supported by a specific authorization by the individual.[4] This authorization (opt-in) requirement, which is addressed in more detail in the next section, effectively means that the default operating procedure for health insurers is to assume that a consumer opts out of, or restricts, data sharing for any purpose not linked to treatment, payment or health care operations or as otherwise required by law (e.g., disclosure to the Department of Health and Human Services pursuant to an investigation or enforcement action).

Furthermore, in order for public policy to be effective at combatting the substance use disorder (SUD) and mental health crisis facing the nation today, policymakers must allow for use and disclosure of SUD and mental health-related information for treatment, payment and health care operations including care coordination. While SUD records have historically been more restricted under federal and state law, there has been an evolution in favor of sharing this information because of reduced stigma. Federal and state policymakers and diverse stakeholders are working in this direction, and there is wide consensus that alignment of substance use disorder information protections with HIPAA is the best path forward (e.g., without requiring special authorization). Pending federal rules would allow covered entities to more freely use and disclose PHI in scenarios that involve SUD, serious mental illness and emergency situations as well as when disclosures are in response to a "serious and reasonably foreseeable threat" in recognition that access to this information will ultimately benefit the patient and their caregivers.[5]

Consumer Notice Requirement for Right to Opt Out: A consumer's right to opt out of (or restrict) data sharing is already required to be communicated under HIPAA. First, if a health insurer has executed a valid authorization to use and disclose PHI for a purpose beyond treatment, payment and health care operations, the valid authorization must provide the individual with a right to revoke their authorization at any time, provided that the revocation is in writing, except in two very narrow circumstances: (1) the health insurer has taken action in reliance thereon; or (2) if the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.[6]

Second, a Notice of Privacy Practices (NPP) is required under HIPAA. This notice, which must be made available to health plan members at the time of enrollment, describes, among other things, the right an individual has to restrict the use and disclosure of their PHI for even core treatment, payment and operations purposes, as provided by the HIPAA Privacy Rule. A health insurer, like any covered entity, is not required to agree to a requested restriction, unless specifically required to by the Privacy Rule. Indeed, health plans must exchange basic member information to providers in order to accurately process claims and keep accurate records on an ongoing basic. Having

[2] 45 C.F.R. §164.502(a).
[3] 45 C.F.R. §§ 164.506 and 164.510.
[4] 45 C.F.R. §164.508.
[5] 86 Fed. Reg. 6446, 6479-84.
[6] 45 C.F.R. §164.508(b)(5).

inaccurate member information would jeopardize the integrity of an audit or oversight of safeguards. A covered entity must agree to restrict a disclosure about an individual to a health plan if the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and the PHI pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full.[7] Health plans also voluntarily honor requests to restrict disclosure of PHI in cases when doing so would respect a member's request for privacy while not hindering health plan operations and record keeping, such as in the case of a younger adult on a family's policy who requests that explanation of benefits (EOBs) are not sent to a parents' residence. In addition to providing the NPP at the time of enrollment, health plans must notify individuals covered by the plan of the availability of the NPP and how to obtain it at least once every three years.

- **Right to opt in of [sic] data sharing:** Under HIPAA, an individual must generally authorize (or opt in to) data sharing if a health plan intends to use or disclose data beyond treatment, payment or operations purposes, is not required by law, and is not otherwise permitted by HIPAA without individual authorization. The purposes for which individual authorization is required is addressed in detail in the Privacy Rule. Specifically, a health insurer must obtain an individual's authorization for:
    1. Marketing purposes, except for a communication in the form of a face-to-face communication or a promotional gift of nominal value
    2. Sale of PHI, in which case the authorization must inform the individual that the health insurer will receive remuneration for the sale
    3. Use or disclosure of psychotherapy notes (relevant exceptions are made to carry out certain treatment, payment or health care operations or in connection with legal actions)[8]

  In other words, the default assumption is that a consumer restricts and, therefore, must opt in to uses and disclosures of PHI that is not essential to the nature of health insurance.

  Consumer Notice Requirement: As mentioned above, a consumer's right to opt in to data sharing by providing an authorization is already required by HIPAA. Further, health insurers must adhere to detailed documentation requirements, such as describing the class of persons who will receive the information, the expiration date of the authorization, the individual's right to revoke the authorization after initially providing it, and the potential for redisclosure of the information by the recipient, among other elements.[9]

  Additionally, the NPP must address an individual's right to opt in to data sharing through authorization. Specifically, the NPP must describe the types of uses and disclosures that require an authorization, state that other uses and disclosures not described in the NPP will be made only with the individual's written authorization, and state that the individual may revoke an authorization.[10]

- **Right to correct information:** Under HIPAA, an individual already has the right to correct (amend) PHI or a record about the individual in a designated record set for as

[7] 45 C.F.R. §164.522(a)(1).
[8] 45 C.F.R. §164.508.
[9] 45 C.F.R. §164.508(c).
[10] 45 C.F.R. §164.520(b)(2)(E).

long as the PHI is maintained in the designated record set.[11] As a covered entity, the health insurer must act on the individual's request for an amendment no later than 60 days after receipt of such a request. Any denial to correct by the health insurer must have a basis authorized by the regulation and be communicated to the individual. If the individual disagrees with the denial, the individual may file a statement and/or a complaint to the health insurer or the Department of Health and Human Services. Otherwise, the information must be corrected in the manner provided in the regulation, such as through informing recipients of the corrected information including business associates.

Consumer Notice Requirement: The HIPAA-required Notice of Privacy Practices described in detail above must address an individual's right to correct information held by the health insurer.[12]

- **Right to delete information:** More information about what is intended by this right to delete information would be helpful to fully respond to this aspect of the Draft Policy Statement. Health insurers need certain PHI to perform the basic functions of the business of insurance including for treatment, payment and health care operations. It would not be practicable to maintain a customer relationship with an individual if the individual could request deletion of his or her information. Further, federal law requires health insurers participating in federal health care programs (e.g., Medicare, Medicaid) to retain information for 10 years. Data might be required to be retained for longer periods because of an ongoing legal action. HIPAA requires a health plan to protect member data for as long as the data is held, thus allowing consumer data to be protected over its lifespan.

  We note that included in the right to correct information under HIPAA is the right to delete information that is not accurate. Additionally, an individual who has provided a specific authorization for uses and disclosures requiring authorization may revoke this authorization at any time.

  Consumer Notice Requirement: The HIPAA-required Notice of Privacy Practices described in more detail above must address an individual's right to correct information held by the health insurer, which includes the right to delete inaccurate information.[13] Individuals are informed of their right to revoke an authorization in the Notice as well.

- **Right of data portability:** There are a few ways in which an individual can obtain and reuse/repurpose his or her information under existing and rapidly evolving federal law. First, under HIPAA, an individual has a right of access to inspect and obtain a copy of PHI about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set. A health insurer must provide the individual with access to the PHI in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual.[14]

[11] 45 C.F.R. §164.526.
[12] 45 C.F.R. §164.520(b)(iv)(D).
[13] 45 C.F.R. §164.520(b)(iv)(D).
[14] 45 C.F.R. §164.524.

Pending federal regulations would further expand the HIPAA-required right of access. The proposed regulations would expressly prohibit a covered entity from imposing unreasonable measures that would impede an individual's right of access. It would also create a separate set of provisions addressing an individual invoking their right to direct electronic copies of PHI, if maintained in an electronic health record, to a third party as required by the HITECH Act.[15]

In addition, beginning on July 1, 2021, certain insured consumers will have near real-time access to certain data pursuant to the Centers for Medicare and Medicaid Services (CMS) interoperability requirements. Medicare Advantage plans, Medicaid managed care organizations, and qualified health plan issuers participating in the Federally-facilitated Exchanges must provide a secure FHIR-based application programming interface (API) available to third-party apps and developers. At the direction of the enrollee, the impacted payers must allow access to this Patient Access API within one business day. The API must include a minimum set of data:

- Adjudicated claims and cost information
- Provider remittances
- Cost-sharing
- Clinical data as defined in USCDI v1 if maintained by the payer
- For Medicare Advantage plans with Part D coverage, they must make available formulary and prescription drugs.
- For Medicaid managed care organizations, they must make available preferred drug lists.[16]

Note that beginning in 2022, a separate requirement under the CMS interoperability rules requires impacted payers to exchange, at a minimum, the USCDI elements v1, at a patient's request, with another payer. The receiving payer must incorporate into the plan's records, thus creating a more longitudinal record for the individual regardless of his or her plan.

Consumer Notice Requirement: The HIPAA-required Notice of Privacy Practices described in more detail above must address an individual's right to inspect and obtain a copy of PHI held by the health insurer.[17]

Right to restrict the use of data: We address an individual's right under HIPAA to restrict the use of data as authorized in 45 C.F.R. §164.522(a) in the sections above regarding "opt-out" and "opt-in" rights. We welcome additional clarity from the Working Group regarding any distinctions intended among these rights.

Consumer Notice Requirement: Similarly, we address consumer notice regarding an individual's right to restrict the use of data above.

[15] See 86 Fed. Reg. 6446 (Jan. 21, 2021), available at: https://www.federalregister.gov/documents/2021/01/21/2020-27157/proposed-modifications-to-the-hipaa-privacy-rule-to-support-and-remove-barriers-to-coordinated-care
[16] See 85 Fed. Reg. 25510 (May 1, 2020), available at: https://www.federalregister.gov/documents/2020/05/01/2020-05050/medicare-and-medicaid-programs-patient-protection-and-affordable-care-act-interoperability-and
[17] 45 C.F.R. §164.520(b)(iv)(D).

In closing, we welcome the opportunity to continue to be a resource to the Working Group regarding HIPAA and its enforcement regime as well as identify subject matter experts that may be useful to the Working Group in considering the Draft Policy Statement and potential model's scope of applicability and alignment with HIPAA.

We would like to thank the Working Group for its consideration to our comments. If you have any questions, please do not hesitate to contact BCBSA's Managing Director for Health Data and Technology Policy Lauren Choi at lauren.choi@bcbsa.com.

Sincerely,

Clay S. McClure
Executive Director, State Relations
Blue Cross Blue Shield Association

Arbor Strategies, LLC

Chris Petersen
804-916-1728
cpetersen@arborstrategies.com

June 7, 2021

Ms. Cynthia Amann
Chair, NAIC Privacy Protections (D) Working Group
Missouri Department of Insurance
301 W High St Rm 530
Jefferson City, MO 65101

Dear Ms. Amann:

I am writing on behalf of a Coalition[1] of health insurers representing some of the country's largest major medical insurers and health maintenance organizations to comment on the NAIC Privacy Protections (D) Working Group's ("Working Group") proposed work plan to review "consumer issues" for potential inclusion in, or amendments to, the various NAIC privacy models. As noted in an earlier letter, the Coalition is concerned about the potential ramifications that these "consumer issues" might have on the health insurance industry, particularly those "consumer issues" that were lifted from provisions of the European Union's General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act ("CCPA"). The health insurance industry is already subject to a robust privacy regulatory scheme. Before layering any additional requirements upon the health insurance industry, the Working Group must have a clear picture of the unintended and the intended consequences, to both the delivery and regulation of health care and insurance, of adding these other requirements.

The United States Department of Health and Human Services ("HHS") recently published comments that share our concerns regarding well-intentioned, but potentially ill-conceived privacy regulation. In the executive summary to its proposed modifications to the HIPAA privacy rule, the HHS specifically warns that when done improperly, privacy rules "could present barriers to coordinated care and case management—or impose other regulatory burdens without sufficiently

[1] CVS Health/Aetna, Anthem, Cigna and UnitedHealthcare, who together provide health insurance and health maintenance organization coverage to more than 200 million members nationwide, are the members of this Coalition.

compensating for, or offsetting, such burdens through privacy protections."[2] HHS also warns that the unintended consequences of privacy rules that fail to consider all of the nuances of our health care system could "impede the transformation of the health care system from a system that pays for procedures and services to a system of value-based health care that pays for quality care."[3]

HHS raises these concerns, in part, because of the unique nature of health insurance, the regulation of health information and the interconnectivity of health insurance, health care providers and the health information that they share. HHS is properly concerned that otherwise well-intentioned regulation of health information could instead harm consumers by negatively impacting the coordination of care and case management. We believe that HHS' concerns regarding unintended consequences highlight and further justifies the NAIC's earlier decision to include a HIPAA privacy safe harbor in its most current privacy model.

The NAIC included a very important and well-established protection for carriers that comply with the federal HIPAA-privacy requirements in Model 672. That model provides that '[I]rrespective 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."[4]

The HIPAA compliance safe harbor provides carriers with the ability to administratively streamline and implement one comprehensive privacy standard across all health information for all states, while at the same time ensuring that consumer information is protected on a consistent basis under the stringent privacy standards established under HIPAA. The HIPAA privacy standards are constantly evolving to meet the current needs of the environment and aim to reflect the most current thinking on protecting consumer information, while at the same time ensuring that no damage is done to the provision and financing of health care, thus providing consumers with the highest privacy and consumer protection standards.

It is also important to note that the HIPAA compliance safe harbor is simply that—a safe harbor. It is a strong, consistent foundation that works well with state oversight. If a carrier is not compliant with HIPAA standards, the safe harbor disappears and the carrier is subject to appropriate state standards and oversight. It is critical that any privacy model that the NAIC develops includes a safe harbor for HIPAA privacy rule compliance.

---

[2] Federal Register, Vol. 86, No. 12, Thursday, January 21, 2021 at page 6447.

[3] *Id.* at page 6447.

[4] Model 672, §21.

The Working Group's Initial Draft Privacy Policy Statement

The Working Group has set out the following topics for consideration:

1. The right to opt-out of data sharing;
2. The right to opt-in of data sharing;
3. The right to correct or amend information;
4. The right to delete information;
5. The right of data portability; and
6. The right to restrict the use of data

The Working Group's work plan provides that after reviewing and considering these topics listed above, and their potential ramifications, it will determine whether these rights should be imposed upon health insurers. We recommend that the Working Group move slowly, and thoughtfully, while considering these issues

As noted above, HHS is concerned with the unintended consequences of well-intentioned privacy regulations. As regulators of the health insurance industry, the members of the Working Group should also be concerned about the possible impact that implementing some of these suggested topics would have on the health insurance industry and the consumers they serve. Many of those topics, while described as "consumer friendly", actually violate existing state consumer protection laws. For example, although it appears that a "right" to have information deleted would be "consumer friendly", actually it likely runs counter to existing state insurance laws to maintain and protect information. These requirements to maintain information are in place to ensure that insurance regulators can, among other things, enforce state insurance consumer protection laws. It also appears that a "right" of information portability i.e., the right to move information from one entity to another, if coupled with a "right" to deletion, also violates insurance laws requiring carriers and regulators to have direct access to information for market conduct, fair trade practices review and other regulatory investigations.

Before addressing the topics above and their potential unintended consequences, we note that each of these areas is improperly expressed as an absolute "right." That is, individuals have the **right** to amend information or the **right** to delete information. *Emphasis added.* Existing insurance privacy laws, for good reason, do not express these actions as absolute "rights". Rather, they are expressed as a right to request an action; e.g., individuals have the right to request their information be amended. This is true for both the HIPAA privacy rule and the NAIC's Model 672. For example, under existing rules, if individuals believe there is inaccurate information in their health insurance files, they may request that this information be amended. However, if after investigation the health insurer determines that the information is accurate, then the health insurer has the right to deny the request to amend the information. In fact, health insurers may actually be required by law to deny the request under state insurance laws mandating those insurers maintain accurate and complete medical information and records.

In addition to the above, we make the following specific comments with respect to each of the subject areas noted above:

The Right to Opt-out of Data Sharing

As we discussed in our earlier letter, the Coalition requests a better understanding of what the "right" to "opt out of data sharing" actually entails before we can competently comment on this issue. There is a range of possibilities. For example, it could mirror the limitations outlined under the GLBA privacy rules, under which individuals are given the right to opt-out of certain disclosures (once again, note that this is not an absolute right, but is limited to certain types of disclosures, and only if certain conditions are met). Model 672, which was designed to implement the GLBA privacy requirements, uses the term opt-out as part of its limitation on disclosures of nonpublic personal financial information to nonaffiliated third parties. It provides that licensees may not, directly or through any affiliate, disclose any nonpublic personal financial information about a consumer to a nonaffiliated third party unless certain requirements are met. Alternatively, the opt-out referenced above could be referring to a right under the HIPAA privacy rule giving individuals the right to request restrictions regarding the use and disclosure of their protected health information as it relates to treatment, payment, or health care operations, and the right of individuals to request restrictions for other disclosures, such as those made to family members, none of which are absolute "rights."[5]

Health plans provide both of the rights described above as part of complying with state and HIPAA privacy laws and health plans must be permitted to continue to craft the clear and precise opt-out rights already provided for under state and federal law. We urge the Working Group to craft an exemption for health carriers that are compliant with HIPAA and applicable state laws.

The Right to Opt-in of Data Sharing

The Coalition also requests a better understanding of what the Working Group intends by the "right" to "opt-in of data sharing" before fully commenting on this issue. Health insurers presently disclose or "share data" under authorizations provided by individuals or as required o permitted by law. Obviously requiring individuals to opt-in to disclosures that are required by law or that are necessary for are the treatment, payment or health care operations would be extremely problematic and would appear to be contrary to public policy.

---

[5] 45 CFR § 164.522

The Right to Correct or Amend Information

Health plans are already subject to a similar requirement under the HIPAA privacy rule. This provision provides that covered health plans must permit individuals to request that the health plan amend protected health information maintained in a designated record set. The rule sets out additional requirements as to when and whether the health plan must amend the information and other procedures.[6] For example, while an individual can request that certain information be removed from a medical record, if that information is correct, then in order that appropriate care be given, it is critical that the information not be deleted or amended. Again, we suggest that health plans that are HIPAA compliant are already providing the appropriate "right" regarding correction or amendment, and should be exempt from any additional regulation which may ultimately hinder the provision of health care and health care financing.

The Right to Delete Information

This subject would appear to conflict with insurance laws requiring health plans to maintain records. State law and NAIC's model acts are full of requirements that health plans maintain records. The NAIC's Unfair Trade Practices Act includes at least three separate provisions that require insurers to maintain records. For example, the Unfair Trade Practices Act includes a provision entitled: 'Failure to Maintain Marketing and Performance Records'. This provision defines an unfair trade practice as the "[f]ailure of an insurer to maintain its books, records, documents and other business records in such an order that data regarding complaints, claims, rating, underwriting and marketing are accessible and retrievable for examination by the insurance."[7] Insurers must maintain this data for at least the current calendar year and the two preceding years. Similarly, the NAIC's Market Conduct Record Retention and Production Model Regulation, by its very title, requires insurers to maintain records. Under the model, insurers are generally required to retain records for at least three years i.e., insurers may not delete records during this protected period.

It also appear that HIPAA's right to amend information, which, as noted above, health insurers are already compliant with, addresses the most obvious benefits that a right to delete information grants to an individual. If there is inaccurate information in a health file, the individual that is the subject of that information can ask that the information be corrected. Individuals, however, should not have the right to have accurate information deleted. Health plans need this information to coordinate care, provide continuity of care and otherwise maintain information that insurance regulators might need to ensure compliance with state laws and regulations.

---

[6] 45 CFR § 164.526

[7] Unfair Trade Practices Model Act, Subsection §4.J.

The Right of Data Portability

Portability, as the term is used in the GDPR and the CCPA, is inappropriate for application to the health insurance industry. These laws define portability as the ability of an individual (data subject) to receive the personal data the individual has provided to a controller and transmit it to another controller without hindrance from the controller that presently has the data. At the heart of this concept is that individuals should be allowed to freely move their own data from one controller (insurer) to another controller (presumably any other business entity that collects data) whenever they want to move the data. As we noted in previous comments, the health insurance industry is not the target of either the GDPR or the CCPA. Rather, their focus is the service and technology industries that collect, compile, and sell consumer information. Rules aimed at Google, Microsoft, Amazon or other large technology companies are not necessarily appropriate for the health insurance industry, and in this case, they clearly are not.

The portability concept operates under the assumption that the individual consumers should be able to decide with whom they conduct business, whose services they want to use and where their information resides. Implicit in the concept is that portability addresses the concern that individuals can be held hostage by the controllers that are in possession of the individual's information so that, for example, an individual would not be able to select a new telephone service provider until the former releases the number, and once the individual has selected a new service provider, the former provider no longer needs the consumer's data. This potential harm does not exist in the health insurance industry. Health insurers do not control their customers by maintaining their health records. Employers and individuals regularly switch insurers, and individuals have the right to freely authorize and direct their information be given to another insurer.

As discussed above regarding the right to delete information, portability rights, if coupled with a deletion requirement, would also appear to conflict with state insurance laws requiring health plans to maintain accurate and complete records. If an individual could direct a health insurer to transmit the individual health and insurance information to another controller without hindrance, and then direct the insurer to delete the information transmitted, it would be impossible for the health insurer to maintain information as required by state law, it would jeopardize continuity of care and would make the maintenance of accurate health records difficult, if not impossible. It also has the potential to make it impossible for state insurance regulators to conduct their market conduct and examination functions if health plans are unable to maintain the records of their policy and certificate holders.

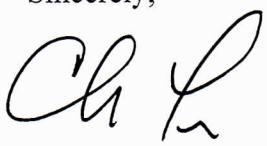
The Right to Restrict the Use of Data

As discussed above, health plans are already subject to the HIPAA privacy rule requirements granting individuals the right to request restrictions regarding the use and disclosure of their protected health information for treatment, payment and operations and the

right of individuals to request restrictions for other disclosures, such as those made to family members. We, therefore, urge an exemption for health plans that already are HIPAA compliant.

Thank you for allowing us to comment. If you have any questions, please feel free to reach out to me at either (202) 247-0316 or cpetersen@arborstrategies.com. We look forward to working with the Working Group as it discusses topics for possible inclusion in a revised NAIC privacy model.

Sincerely,



Chris Petersen

cc: Lois Alexander