BlueCross BlueShield Association

An Association of Independent Blue Cross and Blue Shield Plans

September 7, 2021

Ms. Cynthia Amann, Chair
Mr. Ron Kreiter, Vice Chair
NAIC Privacy Protections (D) Working Group
Attn: Lois Alexander, Market Regulation Manager II

Via email: lalexander@naic.org

RE: First Working Group Exposure Draft of Privacy Policy Statement (Aug. 30, 2021)

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

The undersigned organizations thank you for the opportunity to provide additional input on the Privacy Protections (D) Working Group's (Working Group's) "First Working Group Exposure Draft of Privacy Policy Statement" (referred here as the "Draft Policy Statement") exposed on Aug. 30, 2021. As indicated by the Draft Policy Statement, this is "the framework for the minimum consumer data privacy protections that are appropriate for the business of insurance to be applied to NAIC models #670, #672, etc., as revisions, if possible, or as a start for a new model, if necessary."

We appreciate the Working Group's efforts to include stakeholder feedback, particularly those of the health insurance community, in the Draft Policy Statement and on prior Working Group calls. Informed by our experience, we wish to emphasize and build upon certain recommendations provided previously to the Working Group.

While we understand the Working Group specifically solicits feedback at this time on Segment 1 of the Draft Policy Statement, some of our comments are global in nature or address the Conclusion provided at the end of the Draft Policy Statement. In light of this, we ask the Working Group to consider these general comments across Segments as it continues its work to finalize the Draft Policy Statement by the end of the year.

First, as you know, health insurers have a long-standing commitment to data protection, and our consumers' privacy and consumer trust is foundational to all that we do. We wholeheartedly

agree with the Draft Policy Statement's last statement that "our greatest request is for simplicity and harmonization of consumer data privacy requirements." This is why, as previously discussed, federal laws, primarily the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, and the 2020 Interoperability Final Rules, exist. They create a consistent regime, not just for the health insurance industry, but also the broader health care system. Insurers that are in compliance with this regime adhere to robust existing consumer data privacy protections, which continue to evolve to meet the needs of consumers and the technological advances in the health care sector.[1] Accordingly, we urge the Working Group to preserve the HIPAA compliance exemption and carve out, as established in Model 672, any new recommended requirements that are already addressed by existing federal laws to which health insurers are subject and follow, including any revisions to disclosure requirements. Adding any additional layer of consumer data privacy requirements would be duplicative, confusing to both consumers and health insurers, and add administrative burden and costs without adding meaningful protections for consumers.

To the extent that the final Policy Statement and any eventual model changes are broadly applicable to insurers, such model requirements should defer to existing related requirements under federal law. For example, rather than add new and overlapping consumer disclosure requirements, as suggested in the Conclusion section of the Draft Policy Statement, health insurers should be deemed to have satisfied disclosure requirements if they follow applicable HIPAA-required disclosure requirements (e.g., the Notice of Privacy Practices, providing an accounting for certain disclosures at the consumer's request, and generally obtaining a specific authorization in advance to use and disclose information for purposes outside of treatment, payment, and operations with the right to revoke the authorization at any time).[2]

Alignment with HIPAA will ensure that the same robust privacy protections apply to the same type and use of health information in all jurisdictions. Ultimately, this cross-state consistency will enhance compliance in creating a more unified regime, alleviating unnecessary confusion for consumers, health care providers, and the industry.

Second, we wish to reinforce prior feedback regarding Segment 1, The Right to Opt-Out of Data Sharing, defined as "simply the ability of consumers to retain control of what data can be shared and to whom." Under HIPAA, an individual's written authorization is required for additional uses and disclosures beyond an allowed purpose central to treatment, payment or health care operations or for a policy-based exemption set forth in the Privacy Rule.[3] These significant and stringent protections to bar the use and disclosure of protected health information (PHI) results in the default operating assumption that the individual has opted out of data sharing *unless:* (1)

[1] An example of how HIPAA continues to evolve is exemplified by the recent proposed regulation published Jan. 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 PHI and modernize Notice of Privacy Protection Requirements. 86 Fed. Reg. 6446.
[2] 45 C.F.R. §§164.520, 164.528, and 164.508.
[3] 45 C.F.R. §§164.502(a) and 164.508.

specifically authorized by the individual (who can revoke authorization at any time); or (2) the data in question is subject to narrowly tailored regulations that are implemented to fulfill valid public policy goals, or apply to the function related to the system of treating and financing health care in the United States. Health plans must exchange basic member information with providers in order to accurately process claims and maintain accurate records. Having inaccurate member information would jeopardize the integrity of an audit or oversight of safeguards that could have deleterious impact downstream. In conclusion, the existing HIPAA Privacy Rule regime and state laws should not be displaced by new "opt-out" requirements. We urge the Working Group to maintain an exemption for health insurers that are compliant with HIPAA and applicable state laws.

We appreciate the Draft Policy Statement's inclusion of our previously submitted descriptions for how existing requirements apply in the "Current state/federal laws/rules that apply" subsections within each Segment.[4] Including this information provides valuable context and a basis to support maintaining an exemption for HIPAA-regulated entities from new requirements. We look forward to continuing to engage with you and be a resource to the Working Group regarding HIPAA and its evolving and comprehensive enforcement regime. Our subject matter experts stand ready to be useful to the Working Group in finalizing the Draft Policy Statement and aligning with existing federal law.

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 or Randi Chapman, managing director for state affairs at Randi.chapman@bcbsa.com or Bob Ridgeway, AHIP senior government relations counsel at Bridgeway@AHIP.org.

Sincerely,

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

Bob Ridgeway
Senior Government Relations Counsel
AHIP

[4] For reference, letters from the undersigned organizations are included in the document available at https://content.naic.org/sites/default/files/call_materials/Meeting%20Materials%20-%20June%2014.pdf