From: Choi, Lauren <Lauren.Choi@bcbsa.com>
Sent: Thursday, October 24, 2019 4:52 PM
To: privacyframework <privacyframework@nist.gov>
Cc: Weeks, Harvey B. (Ctr) <harvey.weeks@nist.gov>
Subject: BCBSA comments on NIST Privacy Framework: Preliminary Draft - for submission

Hi, please find attached BCBSA comments on NIST Privacy Framework for submission. Thank you.

_____

Lauren Choi, MA, JD

Managing Director, Health Information Technology

Office of Policy and Representation

Blue Cross Blue Shield Association

1310 G St., N.W.

Washington D.C., 20005

T. 202.626.8639 / M. 202.321.4257

@Laurenchoi10/ Lauren.choi@bcbsa.com

BlueCross BlueShield Association
1310 G Street, N.W.
Washington, D.C. 20005
202.626.4800
www.BCBS.com

October 24, 2019

Submitted via Electronic Mail to: privacyframework@nist.gov

Katie MacFarland
National Institute of Standards and Technology
100 Bureau Drive
Stop 200
Gaithersburg, MD 20899

RE: NIST Privacy Framework: Preliminary Draft Comments

Dear Ms. MacFarland:

The Blue Cross Blue Shield Association (BCBSA) appreciates the opportunity to respond to the National Institute of Standards and Technology's (NIST) proposed Privacy Framework as published in the *Federal Register* on Sept. 9, 2019.[1] BCBSA is a national federation of 36 independent, community-based and locally operated Blue Cross and Blue Shield (BCBS) companies (Plans) that collectively provide healthcare coverage for one in three Americans. For 90 years, BCBS Plans have offered quality healthcare 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.

BCBSA commends the agency's approach of developing the Privacy Framework in partnership with public and private stakeholders and believes the Privacy Framework could help to improve organizations' ability to assess their privacy risks. We also appreciate that the Privacy Framework does not take a one-size-fits-all approach as organizations vary in structure, size, revenue and industry type. Consequently, we believe the Privacy Framework will aid organizations in developing effective privacy programs that meet their specific business needs.

However, the healthcare industry is highly regulated, and those companies within this sector have incorporated many privacy and security protocols within their infrastructure to meet those regulatory requirements. Accordingly, we share the view that the healthcare industry helps serve as an example of successful practices for protecting the privacy and security of personal health information.

[1] 84 Fed. Reg. 47255. The Preliminary Draft and related resources were available on the NIST website at: https://www.nist.gov/privacy-framework/working-drafts.

The NIST Privacy Framework Must Be Voluntary For Entities Regulated By HIPAA

Healthcare entities, including plans and providers, must adhere to a variety of federal and state privacy laws and regulations. These federal laws include, but are not limited to, the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), Gramm-Leach-Bliley Act (GLBA), the Genetic Information Nondiscrimination Act (GINA), and the Confidentiality of Substance Use Disorder Patient Records. Given the complexity and breadth of these regulatory requirements, we endorse the Privacy Framework as a voluntary tool that can assist entities in assessing privacy risks, identifying privacy gaps in current practices, and developing comprehensive, effective privacy programs that take into account innovative approaches to safeguarding individuals' privacy.

Healthcare entities need flexibility when it comes to the implementation of the Privacy Framework to ensure it fits within their privacy programs, which are developed to meet statutory and regulatory mandates. Further, considering the evolving state of privacy laws and regulations, periodic refinements to privacy programs are made to respond to industry threats and best practices. We believe the Privacy Framework can act as a beneficial, voluntary guide when evaluating the shifting landscape of privacy threats and safeguards.

Consequently, we encourage NIST to recognize that the healthcare sector is already heavily regulated, and that these entities should not be mandated to implement the Privacy Framework. Instead, the Privacy Framework should be viewed as a voluntary tool used to supplement existing privacy programs.

The NIST Privacy Framework Should Provide Guidance To Align HIPAA Privacy Safeguards To Those Entities Not Regulated By HIPAA, But Are Receiving Protected Health Data

Many organizations that transmit, create, maintain or receive protected health information are not regulated by any federal or state privacy statutes or regulations. Specifically, mobile devices, social media, the Internet of Things and artificial intelligence are combining in a way that creates a multitude of concerns for individual privacy. As an example, when a consumer directs a plan or provider to transmit claims or treatment information to a third-party mobile application, that application receiving the information is not regulated by HIPAA; however, the entity is permitted to use and disclose the information in a multitude of ways, leaving this information susceptible to uses and disclosures individuals may not know about or understand. As such, when HIPAA is not implicated, very few, if any, federal statutes or regulations govern the privacy of the individual's protected health information.

Consequently, for entities participating in the healthcare sector who are not governed by HIPAA, we encourage NIST to develop further guidance that aligns with and incorporates HIPAA Privacy Rule concepts to help promote better privacy protections of consumers' health information by these non-HIPAA entities. This is highly sensitive information that we believe should be protected in accordance with the existing specific safeguards applicable to HIPAA-covered entities.

BCBSA understands the importance of innovation, but believes individuals also have the right to understand how their protected health information is used and disclosed. As such, we believe that NIST can assist in better protecting health data that falls outside the boundaries of HIPAA by incorporating into the Privacy Framework concepts and guidance that aligns with the HIPAA safeguards.

We thank you for the opportunity to provide comments on these important issues. BCBSA looks forward to an ongoing dialogue that can help better and improve the Privacy Framework. If you have questions or want additional information, please contact Lauren Choi, Managing Director of Health Information Technology Policy at lauren.choi@bcbsa.com or 202.626.8639.

Sincerely,

Kris Haltmeyer
Vice President
Legislative and Regulatory Policy
Blue Cross Blue Shield Association