SUBMITTED ELECTRONICALLY

November 9, 2018

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW
Room 4725
Washington, DC 20230

RE: Docket No. 180821780-8780-01: Privacy Request for Comment

Dear Sir or Madam,

The Confidentiality Coalition respectfully submits these comments in response to the National Telecommunications and Information Administration's request for comment on the Administration's proposed approach to advance consumer privacy while protecting prosperity and innovation (the "Proposed Approach"). The Confidentiality Coalition is composed of a broad group of hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacies, pharmacy benefit managers, health information and research organizations, patient groups, and others founded to advance effective patient confidentiality protections. The Coalition's mission is to advocate policies and practices that safeguard the privacy of patients and healthcare consumers while, at the same time, enabling the essential flow of patient information that is critical to the timely and effective delivery of healthcare, improvements in quality and safety, and the development of new lifesaving and life-enhancing medical interventions. The Coalition's members have adopted nine privacy principles that guide its work and its recommendations, which we have attached as Appendix A to this letter along with additional information about the Coalition and its membership.

COMMENTS

We commend the Administration for expressing its intention to maintain HIPAA and other sectoral privacy laws, and to exempt persons and organizations currently subject to these laws from new privacy requirements.

The Coalition agrees with the Administration that the Proposed Approach should focus on strengthening privacy protections outside of sectors that are currently regulated by federal laws, as the creation of overlapping privacy and security requirements could increase regulatory burden on industries subject to sectoral laws without improving existing privacy protections for individuals.

In the health industry, HIPAA balances individuals' privacy rights while permitting vital uses and disclosures of protected health information to take place. HIPAA specifically permits certain uses or disclosures of the information without the individual's authorization while also giving individuals the ability to exercise control over their protected health information by requiring health care providers and health plans to obtain an individual's authorization prior to using or disclosing such information for other purposes.

Currently, organizations that are subject to HIPAA must also comply with additional federal, state and international privacy and data security laws that are as or more strict than HIPAA. While sometimes these laws align with one another, existing non-alignments create significant burdens for organizations that are subject to HIPAA. For example, 42 C.F.R. Part 2, which applies to certain substance use disorder treatment records, prevents health care providers from sharing such records for treatment purposes without first obtaining written consent. These conflicts between federal, state and international privacy frameworks create barriers to developing interoperable health information networks with providers that are subject to the more stringent laws. For this reason, the Coalition favors legislative solutions that would allow HIPAA to preempt other conflicting federal and state privacy laws.

The Proposed Approach should create consistency so that persons and organizations not covered by HIPAA that create, compile, store, transmit, or use health information operate under a similar expectation of acceptable uses and disclosures.

HIPAA only applies to "covered entities" – health plans, health care clearinghouses, and health care providers that engage in electronic transactions – and to persons or entities that create, receive, maintain or transmit protected health information on behalf of covered entities (i.e., "business associates"). There are many organizations that receive health information from consumers that are not subject to HIPAA because they are neither covered entities nor business associates. For example, application developers that offer innovative applications and tools to permit consumers to track their own health and/or health care are not covered by HIPAA if they offer the application directly to consumers (as opposed to offering the application through a health care provider or health plan).

Consumers do not necessarily appreciate the distinction between activities regulated by HIPAA and activities that would be regulated under the Proposed Approach, and instead may expect that any health information they provide to a third party would be protected by HIPAA or similar privacy protections.

We believe the Proposed Approach can help close the current consumer expectation gap provided that the Administration sets forth sufficient guidance to persons and organizations that handle identifiable health information on what they must do to achieve the privacy outcomes outlined by the Proposed Approach, and such guidance aligns with HIPAA's protections.

The Coalition wishes to highlight the following specific considerations with respect to the privacy outcomes identified by the Administration:

- *Transparency*: Not all consumers may read or understand lengthy notices provided at the initial point of interaction. We believe it is important, however, that consumers be able to quickly and easily obtain information about how an organization collects, stores, uses, and shares their identifiable health information. We support the development of innovative ways to improve consumer understanding of privacy notices, with such notices serving as a common template for communicating the organization's collection and use of identifiable health information. The federal government's adoption of model privacy notices that can be customized based on individual organizations' collection and use of data has helped to make privacy notices in the health and financial services industries more consumer-friendly. In the financial industry in particular, a safe harbor offered under the Gramm-Leach-Bliley Act to entities that use the model consumer-friendly notice has led to almost universal adoption of the model notice.

- *Control*: Under HIPAA, individuals must authorize the use and disclosure of their protected health information outside of treatment, payment, health care operations and certain public health uses and disclosures. Similarly, organizations under the Proposed Approach should be required to provide consumers with reasonable control over the collection, use, storage, and disclosure of their identifiable health information. The level of control required should depend on context, taking into consideration factors such as a user's expectations and the sensitivity of the information. For example, in the context of using data for medical research or analytics, HIPAA permits the use of de-identified data, which protects privacy while supporting important societal goals.

- *Security*: We agree that organizations should be required to take *reasonable* security measures that are appropriate to the level or risk associated with the improper loss of, or improper access to, the collected personal data. But as both security threats and available security measures to mitigate against threats are constantly evolving, a reasonableness standard implemented without guidance or compliance safe harbors will create a moving target for organizations with no assurance that the investments they are making in security are sufficient to meet the reasonableness standard. Additionally, consumers may not be aware of or understand variations in the security safeguards implemented by consumer-facing businesses under a reasonableness standard. The Payment Card Industry Data Security Standard (PCI-DSS) certification is an example of an industry-developed certification aimed at defining industry expectations for data

security. The Administration should consider supporting these industry-led efforts by providing safe harbor protections for organizations that obtain such certifications.

- *Access and Correction:* We agree with the Administration that consumers should have qualified access and the ability to request corrections or amendments to their personal data. HIPAA's structure for ensuring this privacy outcome is instructive. HIPAA permits individuals to obtain access to protected health information used to make decisions about individuals' treatment or payment for their treatment, and to request for amendments or corrections to such information. Covered entities may, however, deny requests for amendment if the information is accurate, provided that they annotate the information to account for the disagreement. In the Administration's description of the "Access and Correction" outcome, the Administration suggests that individuals should also have the ability to request deletion of their personal data. We are concerned that organizations will be unable to adjudicate and comply with requests for deletion, as permanently changing or destroying health information can present safety risks to the individual, and compliance risks to the organization. It is important to ensure that organizations may deny deletion requests when the deletion would jeopardize the consumer's safety or the organization's ability to comply with law.

Overall, we agree with the privacy outcomes identified by the Administration's framework, but ask that the Administration consider how these outcomes would be applied by organizations in the health care context, and provide targeted guidance to ensure consistent application of these outcomes.

The Coalition supports the Administration's proposal to implement a risk and outcome-based approach to privacy, but stresses the importance of the availability of detailed guidance that establishes the expectations for assessing risk and achieving the privacy "outcomes."

Properly done, a risk-based approach provides much-needed flexibility to organizations to implement privacy policies and controls. The success of such an approach, however, depends on the certainty organizations can have that what they are doing to comply with the framework is sufficient. Without such certainty, organizations might find a risk-based approach burdensome – as the process for determining the appropriate privacy controls and policy could be both labor and cost intensive. In the end, the process could reward organizations with weaker controls by minimizing the need for privacy and security investments due to the lack of objective requirements.

We recommend that the Administration seek input from a wide range of industry stakeholders, including stakeholders from HIPAA-regulated entities, to develop guidelines for the proper assessment and mitigation of privacy risks. The Administration should develop and release these guidelines prior to the activation of the Administration's proposed framework.

The Administration should leverage existing definitions from NIST, HIPAA, and the Gramm-Leach-Bliley Act where available as opposed to creating alternative definitions.

NIST, HIPAA, and the Gramm-Leach-Bliley Act all contain helpful definitions for key privacy and data security terms. The goal of the Administration in selecting definitions should be to harmonize the Proposed Approach with existing sectoral laws and industry frameworks rather than to develop a separate set of terms.

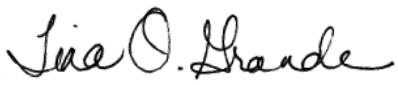
The Coalition supports the Administration's proposal to have the FTC enforce the Proposed Approach, but requests that the Administration direct the FTC to issue enforcement guidance and provide enforcement safe-harbors to organizations that meet the FTC's guidance.

Outside of the sectoral privacy laws enforced by the FTC where the FTC has used rulemaking to establish regulatory requirements (e.g., the Children's Online Privacy Protection Act and the Controlling the Assault of Non-Solicited Pornography And Marketing Act), the FTC otherwise has limited rulemaking authority under the FTC Act. As a result, the FTC generally relies on its enforcement authority to determine when privacy or data security issues constitute unfair or deceptive trade practices. It would be helpful for the FTC to have additional tools to work with the regulated community on privacy and data security. As we have noted above, the FTC should be given the authority to establish safe harbors for compliance, which would help to establish certainty for organizations as they implement the Administration's risk-based framework, while still providing flexibility for other organizations that cannot meet such safe harbors.

Conclusion

The Confidentiality Coalition appreciates this opportunity to provide comments on the Proposed Approach. Please contact me at tgrande@hlc.org or at (202) 449-3433 if there are any comments or questions about the comments in this letter.

Sincerely,



Tina Grande

Enclosures

APPENDIX A

ABOUT THE CONFIDENTIALITY COALITION

The Confidentiality Coalition is a broad group of organizations working to ensure that we as a nation find the right balance between the protection of confidential health information and the efficient and interoperable systems needed to provide the very best quality of care.

The Confidentiality Coalition brings together hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacies, pharmacy benefit managers, health information and research organizations, clinical laboratories, home care providers, patient groups, and others. Through this diversity, we are able to develop a nuanced perspective on the impact of any legislation or regulation affecting the privacy and security of health consumers.

We advocate for policies and practices that safeguard the privacy of patients and healthcare consumers while, at the same time, supporting policies that enable the essential flow of information that is critical to the timely and effective delivery of healthcare. Timely and accurate patient information leads to both improvements in quality and safety and the development of new lifesaving and life-enhancing medical interventions.

Membership in the Confidentiality Coalition gives individual organizations a broader voice on privacy and security-related issues. The coalition website, www.confidentialitycoalition.org, features legislative and regulatory developments in health privacy policy and security and highlights the Coalition's ongoing activities.

For more information about the Confidentiality Coalition, please contact Tina Grande at tgrande@hlc.org or 202.449.3433.

MEMBERSHIP

Adventist Health System
Aetna
America's Health Insurance Plans
American Hospital Association
American Pharmacists Association
American Society for Radiation Oncology
AmerisourceBergen
Amgen
AMN Healthcare
Anthem
Ascension
Association of American Medical Colleges
Association of Clinical Research Organizations
Athenahealth
Augmedix
Bio-Reference Laboratories
BlueCross Blue Shield Association
BlueCross BlueShield of Tennessee
Cardinal Health
Change Healthcare
CHIME
Cigna
City of Hope
Cleveland Clinic
College of American Pathologists
ConnectiveRx
Cotiviti
CVS Health
Datavant
dEpid/dt Consulting Inc.
Electronic Healthcare Network Accreditation Commission
EMD Serono
Express Scripts
Fairview Health Services
Federation of American Hospitals
Franciscan Missionaries of Our Lady Health System
Genetic Alliance
Genosity
Healthcare Leadership Council
Hearst Health
HITRUST
Intermountain Healthcare
IQVIA
Johnson & Johnson
Kaiser Permanente
Leidos
LEO Pharma
Mallinckrodt Pharmaceuticals
Marshfield Clinic Health System
Maxim Healthcare Services
Mayo Clinic
McKesson Corporation
Medical Group Management Association
Medidata Solutions
Medtronic
MemorialCare Health System
Merck
MetLife
National Association of Chain Drug Stores
National Association for Behavioral Healthcare
NewYork-Presbyterian Hospital
NorthShore University Health System
Novartis Pharmaceuticals
Novo Nordisk
Pfizer
Pharmaceutical Care Management Association
Premier healthcare alliance
Privacy Analytics
Sanofi US
SCAN Health Plan
Senior Helpers
State Farm
Stryker
Surescripts
Texas Health Resources
Teladoc
UCB
UnitedHealth Group
Vizient
Workgroup for Electronic Data Interchange
ZS Associates

CONFIDENTIALITY COALITION

PRINCIPLES ON PRIVACY

1. Confidentiality of personal health information is of the utmost importance in the delivery of healthcare. All care providers have a responsibility to take necessary steps to maintain the trust of the patient as we strive to improve healthcare quality.

2. Private health information should have the strictest protection and should be supplied only in circumstances necessary for the provision of safe, high-quality care and improved health outcomes.

3. The framework established by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule should be maintained. HIPAA established a uniform framework for acceptable uses and disclosures of individually-identifiable health information within healthcare delivery and payment systems for the privacy and security of health information.

4. The Privacy Rule requires that healthcare providers and health plans use the minimum necessary amount of personal health information to treat patients and pay for care by relying on patients' "implied consent" for treatment, payment of claims, and other essential healthcare operations. This model has served patients well by ensuring quick and appropriate access to medical care, especially in emergency situations where the patient may be unable to give written consent.

5. Personal health information must be secured and protected from misuses and inappropriate disclosures under applicable laws and regulations. Strict enforcement of violations is essential to protect individuals' privacy.

6. Providers should have as complete a patient's record as necessary to provide care. Having access to a complete and timely medical record allows providers to remain confident that they are well-informed in the clinical decision-making process.

7. A privacy framework should be consistent nationally so that providers, health plans, and researchers working across state lines may exchange information efficiently and effectively in order to provide treatment, extend coverage, and advance medical knowledge, whether through a national health information network or another means of health information exchange.

8. The timely and accurate flow of de-identified data is crucial to achieving the quality-improving benefits of a national health information exchange while protecting individuals' privacy. Federal privacy policy should continue the HIPAA regulations for the de-identification and/or aggregation of data to allow access to properly de-identified information. This allows researchers, public health officials, and others to assess quality of care, investigate threats to the public's health, respond quickly in emergency situations, and collect information vital to improving healthcare safety and quality.

9. To the extent not already provided under HIPAA, privacy rules should apply to all individuals and organizations that create, compile, store, transmit, or use personal health information. A similar expectation of acceptable uses and disclosures for non-HIPAA covered health information is important in order to maintain consumer trust.